HP StorageWorks

Advanced Web Tools 7.4.x administrator guide

Advanced Web Tools 7.4.x administrator guide

Contents

Tables

About this guide

This document is intended to assist fabric administrators to monitor and modify their HP StorageWorks Multi-protocol Router (MP Router) from a web-based graphical user interface (CLI).

Intended audience

This guide is intended for system administrators and technicians who are experienced with the following:

- HP StorageWorks Fibre Channel Storage Area Network (SAN) switches

- XPath Operating System (XPath OS) 7.4.x or earlier

Related documentation

Documentation, including white papers and best practices documents, is available on the HP web site:

http://www.hp.com/country/us/eng/prodserv/storage.html

To access current Fabric OS 7.4.x documents:

1. Locate the **IT storage products** section of the web page.
2. Under **Networked storage**, click the **SAN Infrastructure** subsection.
3. From the **SAN Infrastructure** web page, locate the **SAN Infrastucture products** section.
4. Click **Multi-protocol Routers and Gateways**.
5. To access XPath OS 7.4.x documents (such as this document), click **B-Series Multi-Protocol Router**.
   The **HP StorageWorks B-Series Multi-Protocol Router** overview page opens.
6. Go to the **Product Information section**, located on the right side of the web page.
7. Click **Technical documentation**.
8. Follow the onscreen instructions to download XPath OS 7.4.x documents.

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Medium blue text: Figure 1	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	• Key names • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and checkboxes
Italics font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Text typed at the command line
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of file and directory names, system output, code, and text typed at the command line

⚠ **WARNING!**   Indicates that failure to follow directions could result in bodily harm or death.

△ **CAUTION:**   Indicates that failure to follow directions could result in damage to equipment or data.

🖉 **IMPORTANT:**   Provides clarifying information or specific instructions.

🖉 **NOTE:**   Provides additional information.

Rack stability

⚠ **WARNING!**   To reduce the risk of personal injury or damage to equipment:
- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install stabilizing feet on the rack.
- In multiple-rack installations, secure racks together.
- Extend only one rack component at a time. Racks may become unstable if more than one component is extended.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site: http://www.hp.com/support/.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

For continuous quality improvement, calls may be recorded or monitored.

HP strongly recommends that customers sign up online using the Subscriber's choice web site: http://www.hp.com/go/e-updates.

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate the products by selecting **Business support** and then **Storage** under Product Category.

HP-authorized reseller

For the name of the nearest HP-authorized reseller:

- In the United States, call 1-800-282-6672.
- Elsewhere, visit the HP web site: http://www.hp.com. Then click **Contact HP** to find locations and telephone numbers.

Helpful web sites

For other product information, see the following HP web sites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.hp.com/support/
- http://www.docs.hp.com

1 Introducing Advanced Web Tools

This chapter provides an overview of HP StorageWords XPath OS Advanced Web Tools, its basic features, components, page contents, and layout. Also included are basic instructions for using Advanced Web Tools. This chapter contains the following sections:

- Advanced Web Tools advantages and capabilities, next
- Supported operating systems and browsers, page 12
- Supported platforms, page 12
- Launching Advanced Web Tools, page 13
- Switch Explorer, page 13
- Switch Manager, page 15
- Logging in to perform administrative tasks, page 18

Advanced Web Tools advantages and capabilities

Advanced Web Tools is a graphical user interface (GUI) that enables administrators to monitor and manage fabrics, switches, and ports from a standard workstation. It is an optionally licensed product that runs on the XPath OS.

Advanced Web Tools provides the administrative control point for fabric services, such as zoning, trunking, and performance monitoring. Advanced Web Tools also provides an interface to telnet commands to perform special switch functions and diagnostics that are available only through the telnet interface.

Advanced Web Tools has two components: *Switch Explorer* and *Switch Manager*. These components run in a web browser on a host connected to an MP Router through a private intranet or the Internet. Switch Explorer and Switch Manager are described later in this chapter.

NOTE: You can access MP Routers simultaneously from different connections (for example, Advanced Web Tools, CLI, and API). If you do this, changes from one connection might not be updated to the other, and some modifications might be lost. Make sure, when you connect with simultaneous multiple connections, that you do not overwrite the work of another connection.

Advantages

Advanced Web Tools is an excellent partner to the traditional XPath OS CLI, and in many ways it can provide faster and more effective results than can be achieved through the CLI.

The following are some of the features that make Advanced Web Tools an important part of the switch management and administration process:

- It is easy to use and has an intuitive interface.
- It can be used from a standard workstation.
- It allows you to be "in front" (virtually) of any fabric, switch, or port.
- It makes zoning a simple "click" process, rather than requiring you to enter world wide names (WWNs) and port numbers to create a zoning configuration.
- It provides a performance monitoring interface, enabling you to the view status and traffic on a switch or port in seconds by creating a variety of graphs.

Capabilities

The following are some of the tasks you can perform using Advanced Web Tools:

- Monitor and manage the entire fabric.
- View fabric-level information, such as the existence of other MP Routers or switches in the fabric.
- Configure and administer the MP Router.
- View information about devices in the fabric.
- Monitor switch hardware component status.
- Configure and manage ports in the fabric, including EX_Ports on the MP Router.
- Manage zone-related objects, such as zones, zone aliases, and zone configurations.
- Filter and monitor switch event logs.
- Monitor port status and performance, including frame counts (frames in, frames out) and error counts.
- Monitor and manage Fibre Channel routing.

Supported operating systems and browsers

Table 2 lists supported operating systems and identifies the browsers and Java™ Plug-ins that can be used on the operating systems.

Table 2   Supported operating systems

Operating system	Browser	Java Plug-in
RedHat Linux® 9.0	Mozilla 1.6	1.4.2_06
Solaris 2.8	Mozilla 1.6	1.4.2_06
Solaris 2.9	Mozilla 1.6	1.4.2_06
Windows® 2000	Internet Explorer 6.0	1.4.2_06
Windows 2003	Internet Explorer 6.0	1.4.2_06
Windows XP®	Internet Explorer 6.0	1.4.2_06

Adequate RAM is required on Windows systems, as follows:

- 128 MB or more of RAM for fabrics comprising 10 switches or fewer
- 256 MB or more of RAM for fabrics comprising 11 to 15 switches or fewer
- 512 MB or more of RAM for fabrics comprising more than 15 switches

HP also recommends a minimum of 8 MB of video RAM.

Supported platforms

Advanced Web Tools is part of the firmware of an MP Router. When you log in to Advanced Web Tools on an MP Router, you can manage other MP Routers in the fabric. When accessing these MP Routers, you are opening the remote MP Router's version of Advanced Web Tools; the functionality available for these MP Routers might vary.

From Advanced Web Tools, you can also manage other HP (non-MP Router) switches. When accessing these switches, you are opening the remote switch version of Fabric OS Advanced Web Tools, rather than the XPath OS version. See the *HP StorageWorks Fabric OS 5.x Advanced Web Tools administrator guide* for more information on this management interface.

Launching Advanced Web Tools

You can launch Advanced Web Tools after the Java Plug-in and web browser are installed and configured on the client workstation. See Table 2 on page 12 for the supported Java Plug-in.

1. Launch the web browser and enter the IP address of the MP Router in the Location/Address box:

   `http://123.123.123.123`

2. Press **Enter**.

3. If the MP Router does not have an Advanced Web Tools license, you are prompted to enter one (see Figure 1).

   a. Enter the license key.

   b. Click **Add License**.

Advanced Web Tools is launched, displaying the Switch Explorer.

Figure 1 Prompt for missing Advanced Web Tools license

Switch Explorer

The first thing you see when you connect to a switch with Advanced Web Tools is the Switch Explorer (shown in Figure 2). The Switch Explorer is divided into several areas that provide access to and information about the fabric. You should familiarize yourself with these areas, as the procedures in this guide refer to them:

- Fabric tree displays a list of all the switches in the fabric.
- Fabric toolbar provides access to fabric-wide services: fabric events, topology, Name Server, and zoning.
- Switch View displays an interactive graphical representation of the selected switch.

  The Switch View shows small circles that mimic the LEDs on the physical hardware (indicating port speed and topology). Under Advanced Web Tools, these small circles never change; instead, you can click on any port to get information about the port speed and topology.

- The Switch View button menu displays buttons that provide switch information, such as status, event information, access to telnet, switch performance, and beaconing.
- Switch information view displays information about the switch, including name, status, operating system version, domain ID, IP address, WWN, and current zone configuration.
- Status legend defines the meaning of the colors visible in the background of various icons in the Switch Explorer.
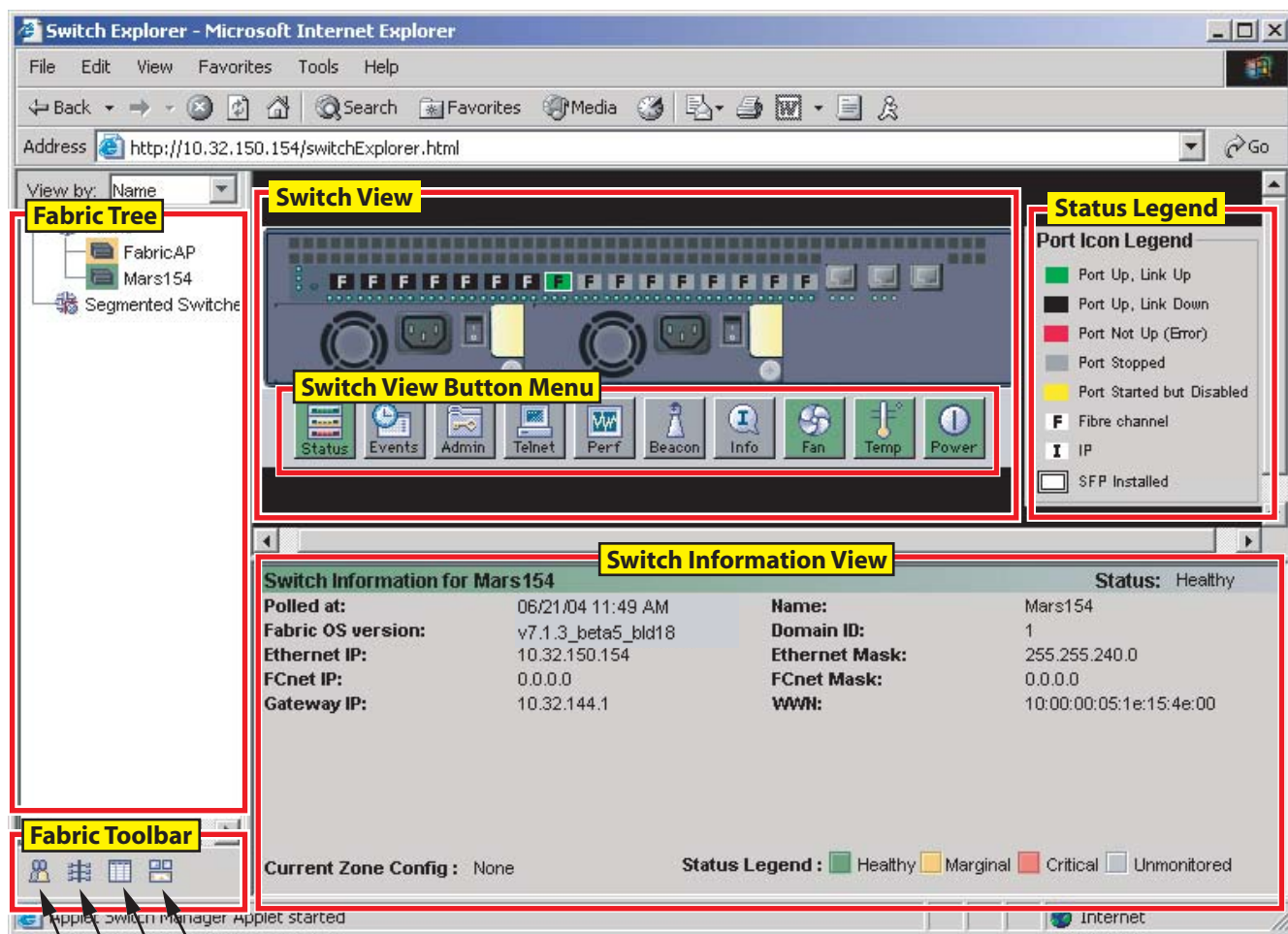
Figure 2 Switch Explorer main window

Supported switches

The fabric tree of the Switch Explorer main window displays all switches in the fabric, including those that do not have an Advanced Web Tools license. However, only MP Routers that have an Advanced Web Tools license and HP StorageWorks switches that have an Advanced Web Tools license installed can be managed through Advanced Web Tools.

If you click a switch in the fabric tree that does not have an Advanced Web Tools license, that switch is not displayed in the Switch View of the Switch Explorer main window. You must either add the Advanced Web Tools license to the switch, or manage the switch through the CLI or through another management application.

Accessing Switch Manager

Switch Explorer also provides access to the Switch Manager component of the interface. Click the following buttons or icons to open a Switch Manager window for the selected MP Router.

📝 **NOTE:** Switch Manager is launched only for MP Routers. For other HP StorageWorks switches, a Fabric OS Advanced Web Tools window is launched. See the *HP StorageWorks Fabric OS 5.x Advanced Web Tools administrator guide* for information on using this interface.

- Any port icon in the switch view
- The following fabric toolbar icons:

  Topology icon

  Name Server icon

  Zone administration icon

- The following switch view buttons:

  Switch events button

  Switch administration button

  Performance monitoring button

Switch Manager

The Switch Manager component of Advanced Web Tools provides more detailed information about the MP Router shown in the Switch View. Figure 3 shows an example of the Switch Manager window.

Caption Bar   Title Bar   Tabs   Task Bar   Navigation Buttons
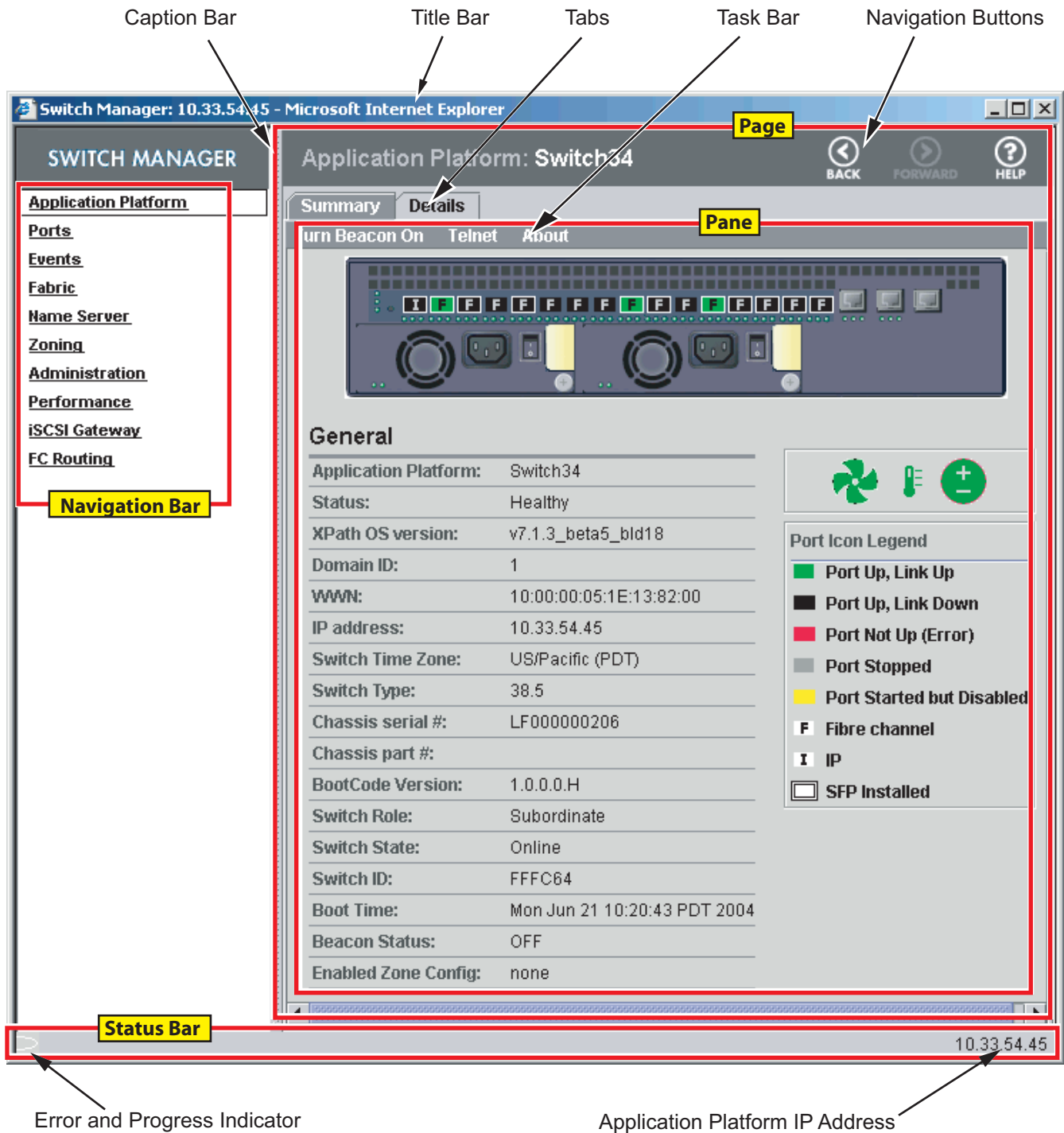
Figure 3 Switch Manager main window and components

Switch Manager enables you to access, configure, monitor, manage, and dynamically interact with the MP Router. Most tasks are performed using Switch Manager.

See "Accessing Switch Manager" on page 15 for information on how to launch Switch Manager from a Switch Explorer window.

The Switch Manager window is divided into several areas that provide access to and information about the MP Router and the fabric. You should familiarize yourself with these areas; the procedures in this guide refer to them:

- Main window: Switch Explorer and Switch Manager each have a main window that exists for as long as the component instance is running; they cannot be closed without quitting that instance of the application. The title bar of the main window indicates which component of the GUI is running in that window. If you quit the Switch Explorer instance, the Switch Manager continues to execute (and vice versa).
- Navigation bar: The navigation bar is located on the left side of the window and provides access to management interfaces, such as Name Server, events, and zoning administration. Clicking an item in the navigation bar displays the corresponding page in the Switch Manager main window.
- Pages: Switch Explorer and Switch Manager display information in *pages*. Pages are displayed in the main window. A page can contain a table or other information. A page may also contain *tabs*. Tabs are usually at the top of a page and provide a categorized view of information about objects shown on the page. You can click a tab to view the display for that tab. There are two types of pages:
  - *Top-level pages* are listed in the navigation bar. A page is displayed in the main window and cannot be closed unless you select another page or quit the GUI application. When a page is selected and displayed, the page name is highlighted in the navigation bar. To go to another top-level page, click the page title in the navigation bar.
  - *Drill-down pages* provide more detail about an object. You can open a drill-down page by clicking a blue, underlined hyperlink. A port drill-down page can also be opened by clicking a port icon. When you open a drill-down page, the page topic is added as a child page under the appropriate parent (top-level) page option in the navigation bar (see Figure 4).

    You can close a drill-down page by clicking the X in the upper right corner of the page. This results in the child page title being removed from the navigation bar.
- Panes: Page tab contents are displayed in *panes*. A pane is the portion of the page display that changes when you click a tab. Panes can contain any or all the elements of a page.
- Tables (not illustrated): Many pages and panes contain tables of information. You can click a column head in a table to sort the order of the table rows according to the entries in that column.
- Hyperlinks: When an item is displayed in blue underlined text, you can click it to open the drill-down page to see more detailed information about that item. For example, in Figure 3 on page 16, the enabled zone configuration name is a hyperlink that, when clicked, opens the zone configuration drill-down page.
- Caption bar: This is at the top of each window; it displays the title for the current top-level page.
- Navigation buttons: Three navigation buttons are at the top right of each window:
  - Back (<): Click to return to the previous page. It is grayed out if there is no previous page.
  - Forward (>): Click to return to pages from which you have navigated using the Back button. It is grayed out if there is no next page.
  - Help (?): Click to display context-sensitive instructions on how to use the current page, pane, or window.

  The Back and Forward buttons navigate between pages, but not between tabs on the same page.
- The task bar is below the page tabs and contains *option buttons* for the operations you can perform from that page. Typically, clicking an option button displays a dialog box, which guides you through the selected operation. Some task bar buttons are always enabled, some are enabled only when you have selected items on the page, and some are enabled only when certain conditions are met for the items selected. (For example, the Start Port task button is enabled only if the selected port is stopped.)
- The status bar is at the bottom of the window; it is divided into three sections:
  - Error and progress indicator: This is on the left side of the status bar. When Switch Manager is sending data to or retrieving data from the MP Router, this indicator is animated. The indicator turns red if there are any errors during the retrieval process. Clicking this indicator opens the Error Log window.
  - Error messages (not illustrated): Error messages are displayed in the middle portion of the status bar. Error messages are automatically cleared after displaying for 10 seconds. You can use the Error Log window to retrieve old error messages.

- MP Router IP address: The right section of the status bar lists the MP Router to which this instance of Switch Manager is connected and, if you are logged on, your user ID.

Drill-down page is a subtopic to parent page   Click here to close the drill-down page
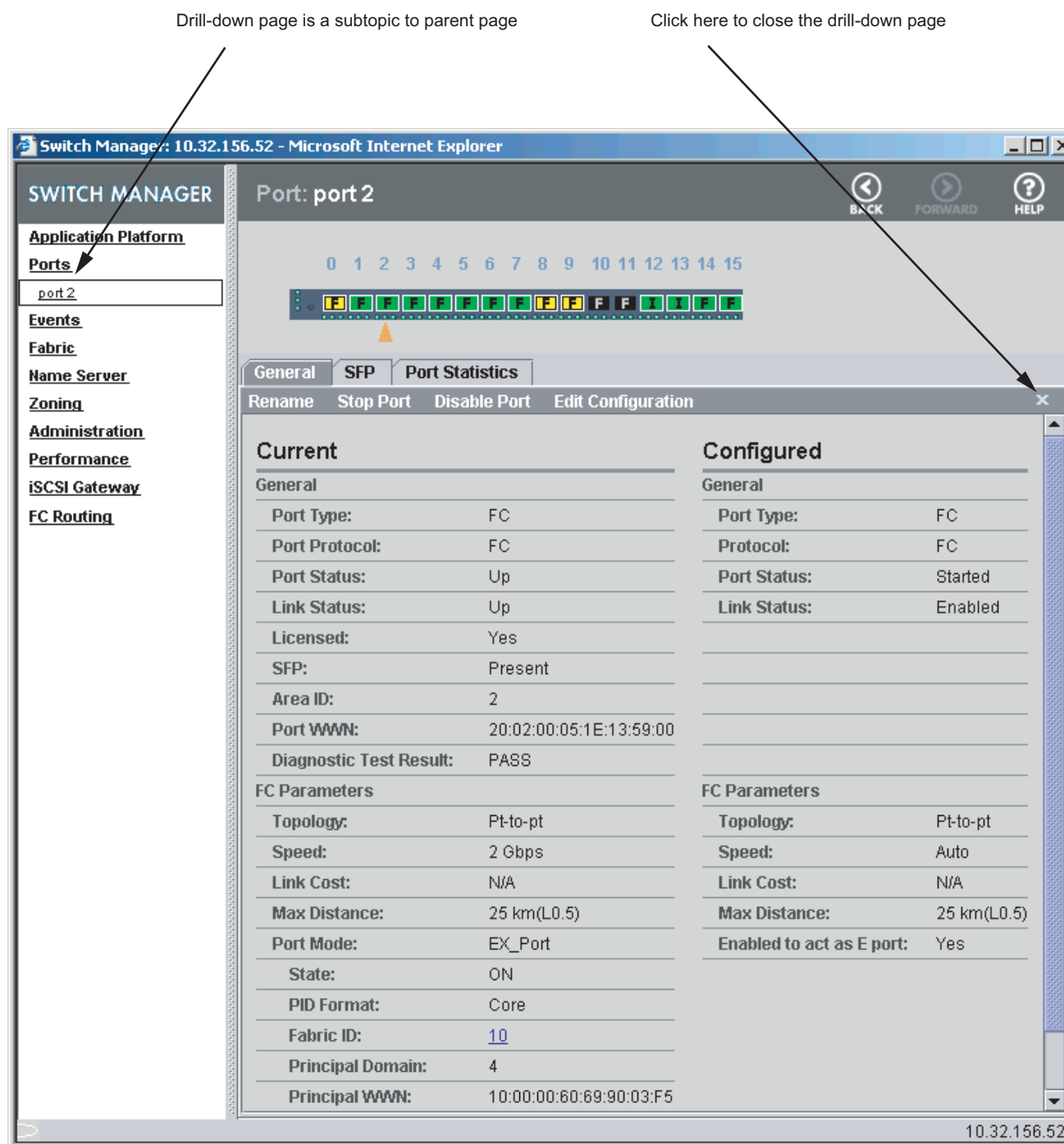
Figure 4 Port drill-down page

Logging in to perform administrative tasks

Switch Explorer and Switch Manager support multiple user accounts and two user roles or permission levels: *admin* and *user*.

You need not log in to either Switch Explorer or Switch Manager to view most displays. However, to perform any administrative task resulting in a change to the system, you must first log in with admin privileges. The first time you attempt to perform a task for which you need admin privilege, an Authorization dialog box opens, asking whether you want to log in and continue.

NOTE: This login behavior is different from Fabric OS Advanced Web Tools, which requires you to log in before you can view the Switch Admin page. XPath OS Advanced Web Tools permits you to browse more information (primarily zoning and port configuration information), without being prompted for a password, than Advanced Web Tools on Fabric OS switches.

If you are logged in with the user role, some options are grayed-out and inaccessible.

Logging in as admin

1. Click **Yes** in the Authorization dialog box.

   The Login window opens.
2. Enter a user name with admin privileges in the User box.

   The default is `admin`.
3. Enter the password for the account in the Password box.
4. Click **OK**.

2 Managing fabrics

This chapter contains procedures for monitoring and managing fabrics, including:

- Viewing fabric information, next
- Configuring fabric parameters, page 22
- Configuring the fabric, page 26

Viewing fabric information

You can view fabric information through the Switch Manager. Click **Fabric** in the navigation bar to access the Fabric page, shown in Figure 5. The Fabric page displays fabric domain information. This page contains two tables.

The Domains table lists all the domains in the fabric. This table contains the following information:

- The name of the switch. This is also a hyperlink leading to subsequent pages, depending on the nature of the device platform:
  - If this is the MP Router managed by this Switch Manager, the hyperlink leads to the Switch Manager Application Platform page for that MP Router.
  - If this is another switch in the fabric, the hyperlink opens another browser window that attempts to connect to that switch. For an MP Router, this results in a new Switch Explorer instance being launched from that MP Router. For other switches, the behavior depends on the type of switch.
- The domain ID for the switch. Every switch in the fabric has a unique domain ID.
- The version of the operating system running on this switch. For MP Routers, this is the XPath OS version; for other HP StorageWorks switches, this is the Fabric OS version.
- The WWN for the switch. The WWN uniquely identifies the switch.
- The IP address of the switch.
- The switch role. This can be either principal or subordinate. (The principal switch is the first switch to boot up in a fabric.)
- For MP Routers, the "FC Router" column will be marked as "Yes."
- IFCS, which displays the status of IP service fabric configuration server (IFCS) switches in the fabric. Status can be Primary, Secondary, Standalone, or N/A (indicating that the switch is not IFCS-capable).

The Topology table contains information about the fabric topology, as seen by the local MP Router. The fabric topology consists of a list of all domains that are part of the fabric and the egress port for each domain.

To reach a certain domain, frames addressed to that domain are forwarded from one port (the ingress port) to another port (the egress port) by the MP Router. The egress port defines the next hop for the frame.

The Topology table displays the following information:

- Remote Domain. The domain ID of a remote switch in the fabric. This is a hyperlink to that switch. Clicking it opens another browser window that connects to that switch. For an MP Router, this results in a new Switch Explorer instance being launched from that MP Router. For other switches, the behavior depends on the type of switch.
- Remote Switch Name. The name of a remote switch in the fabric. This is a hyperlink to that switch; it is the same as the Remote Domain hyperlink.
- Out Port Name. The name of the port on the local MP Router that is connected to the remote domain. This is a hyperlink to the port drill-down page.
- Out Port #. The port number for the port on the local MP Router that is connected to the remote domain.
- # Hops. The number of hops between the local MP Router and the remote domain.
- Link Cost. The cost of the link (for routing decisions).
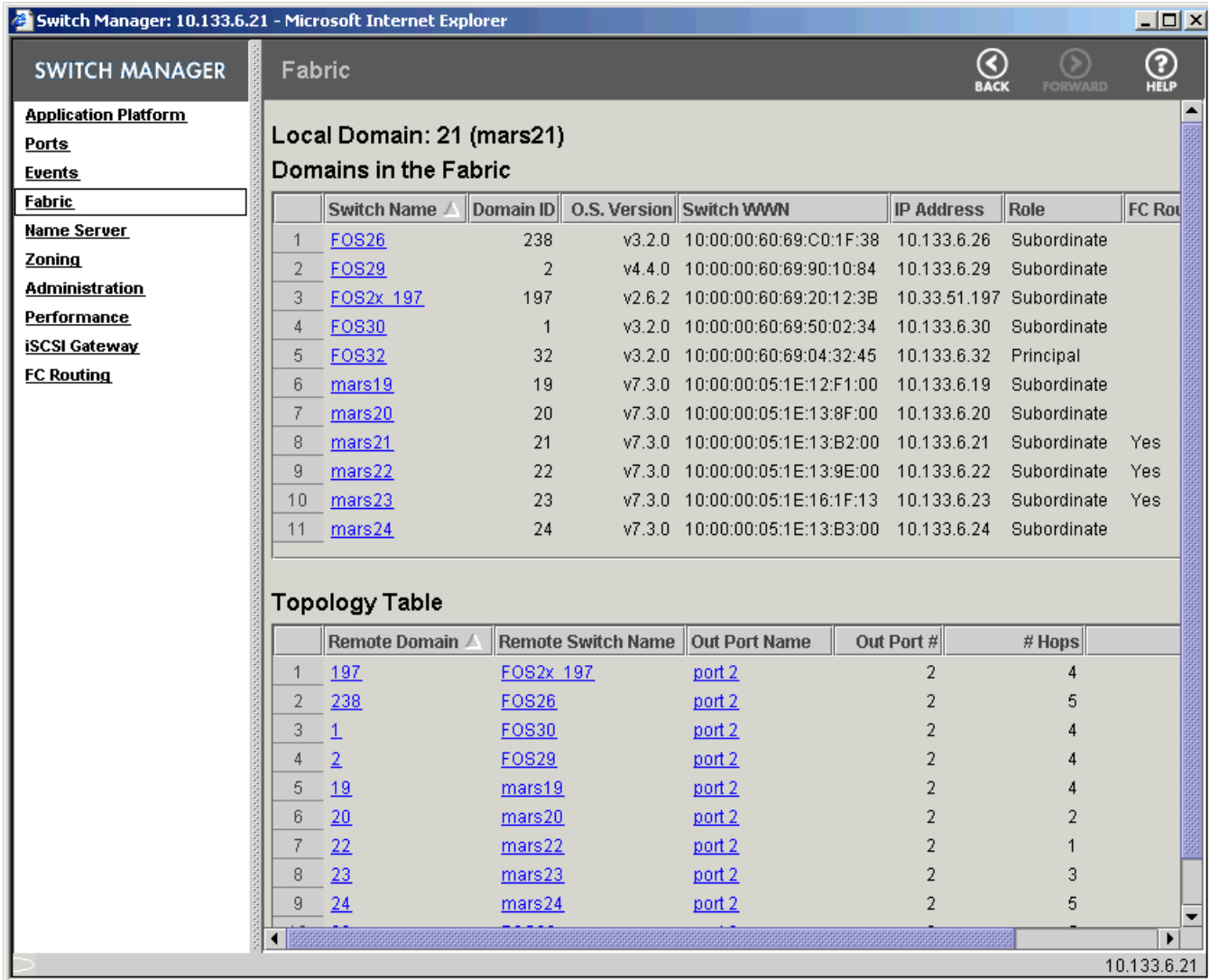
Figure 5 Fabric page

Configuring fabric parameters

It is important to have consistent fabric configuration settings on switches within the same fabric, because inconsistent parameters can cause fabric segmentation.

The Configure Fabric tab on the Administration page (see) allows you to view and configure the following fabric parameters:

⚠ **CAUTION:** Be careful if you change the fabric parameter default values. The fabric might not work correctly if the default values are changed.

- Domain ID: The domain number uniquely identifies the switch in a fabric. This value is automatically assigned by the fabric if you do not configure it.
- BB credit: The buffer-to-buffer credit represents the number of buffers available to attached devices for frame receipt. The range of allowed values is 1 through 32.
- R_A_TOV: The resource allocation timeout value in milliseconds. This variable works with the variable E_D_TOV to determine the actions of the switch when presented with an error condition.

  Allocated circuit resources with detected errors are not released until the time value has expired. If the condition is resolved prior to the timeout, the internal timeout clock resets and waits for the next error condition.

- E_D_TOV: Error detect timeout value in milliseconds. This timer flags a potential error condition when an expected response is not received (an acknowledgment or reply in response to packet receipt, for example) within the set time limit. If the time for an expected response exceeds the set value, then an error condition is met.
- Data Field Size: This specifies the largest possible value, in bytes, for the size of the data frame. The switch advertises this value to other switches in the fabric during construction of the fabric and to other devices when they connect to the fabric.

△ **CAUTION:**   Setting the data field size to a value less than 2112 might result in decreased performance.

- PID Format specifies the port ID format, which is either Core or Extended Edge.
- WAN_TOV: Wide area network timeout value in milliseconds. This is the maximum frame timeout value for a WAN interconnecting the Fibre Channel islands. The value can be 0 or from 1000 through (R_A_TOV / 4).
- MAX_HOP_COUNT: The maximum number of hops a frame might have to take to reach any destination port from any source port across the fabric. The value ranges from 7 to 19.
- RSCN Transmission Mode: The transmission mode of Registered State Change Notification (RSCN) Extended Link Service (ELS) to the end devices. Possible values are:
  - Single PID per payload
  - Multiple PID per payload
  - Fabric format only

The MP Router must be disabled before you make any changes to the fabric parameters. You can either explicitly disable it, or Advanced Web Tools can automatically disable and re-enable it.

Use the following procedure to configure fabric parameters:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Configure Fabric** tab.

   The system configuration settings are displayed (see Figure 6).
4. Click **Edit**.

   The Edit Fibre Channel Configuration dialog box opens.
5. Make the fabric configuration changes in the dialog box.
6. Click **OK**.

   If the MP Router is enabled, Advanced Web Tools disables it before changing the fabric parameters and re-enables it afterward.
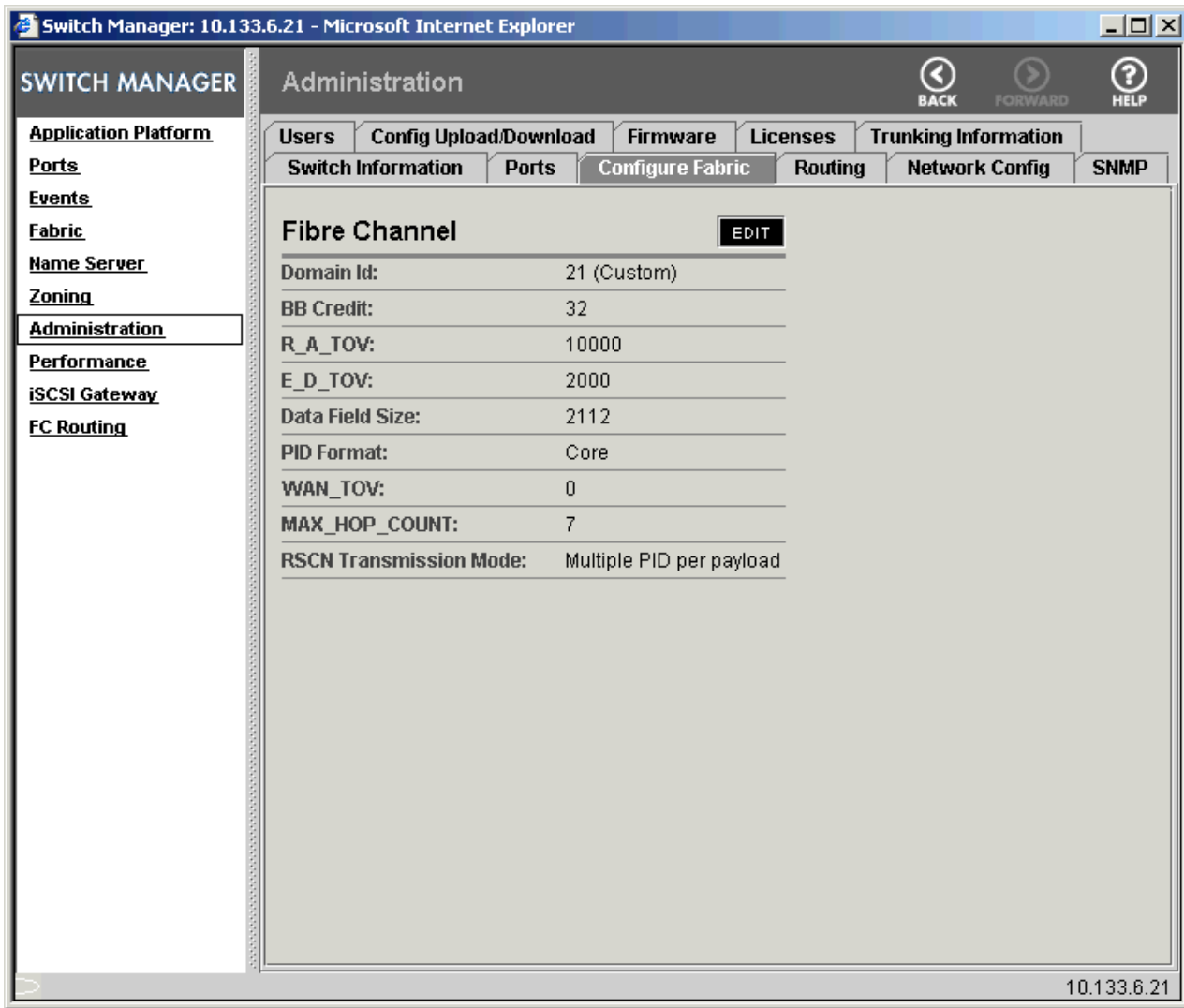
Figure 6 Administration page with Configure Fabric tab selected

Backing up the fabric configuration settings

Keep a backup file of the fabric configuration settings in case the configuration is lost or unintentional changes are made.

> **NOTE:** System configuration parameters vary, depending on switch model and configuration.

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Config Upload/Download** tab (see Figure 7).
4. Verify that the FTP service is running on the host workstation.
5. Click **Upload Configuration** in the task bar.
6. Optional: Click **Edit Server** to make any changes to the configuration file and server.
   The configuration file and configuration server are those listed on the Config Upload/Download pane.
7. Click **OK** to upload the configuration file from the MP Router to the configuration server.
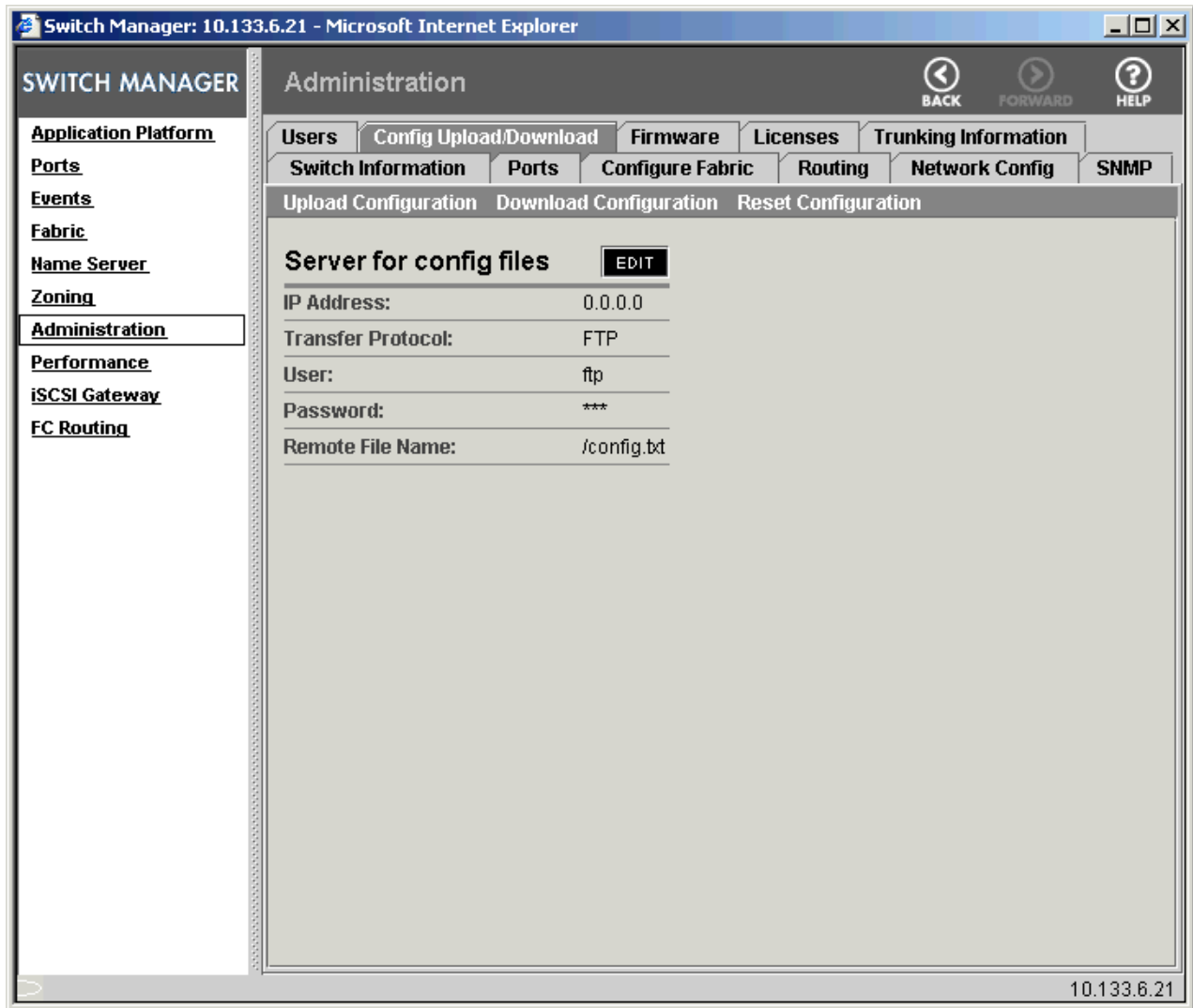
Figure 7 Administration tab with Config Upload/Download tab selected

Restoring previous fabric configuration settings

This procedure restores the system configuration settings from a previously saved backup. The configuration takes effect at the next reboot.

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Config Upload/Download** tab (see Figure 7).
4. Verify that the FTP service is running on the host workstation.
5. Click **Download Configuration** in the task bar.
6. Optional: Click **Edit Server** to make any changes to the configuration file and server.

   The configuration file and configuration server are those listed on the Config Upload/Download pane.
7. Click **OK** to download the configuration file from the configuration server to the MP Router.

Resetting the fabric configuration settings

This procedure resets the fabric configuration settings to their default values. All system parameters are reset to defaults except the following:

- Ethernet MAC address
- IP address
- Subnetmask

- IP gateway address
- License keys
- WWNs
- Zoning configuration
- User accounts and passwords
- Simple Network Management Protocol (SNMP) configurations

Use the following procedure to reset the fabric configuration settings:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Config Upload/Download** tab (see Figure 7 on page 25).
4. Click **Reset Configuration** in the task bar.
5. Click **OK**.

    The switch is rebooted using system configuration default values.

Configuring the fabric

This section provides several procedures for configuring switches in the fabric to ensure connectivity.

Setting the PID format

XPath OS uses either core PID format (the default) or extended-edge PID format. All switches in a fabric must be configured to use the same PID format, or the fabric will segment.

📝 **NOTE:**   When an MP Router is used as a Fibre Channel router (FC router), the MP Router PID format (for the F_Ports and E_Ports) does not need to match the PID format for the attached fabrics. The PID format configured for the EX_Port, however, must match the PID format of the attached fabric. The PID formats of each edge fabric can be different from each other.

---

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Configure Fabric** tab (see Figure 6 on page 24).
4. Verify the PID format in the table.
5. Click the **Edit** button.

    The Edit Fibre Channel Configuration window opens.
6. Select the PID format from the drop-down list.
7. Click **OK**.

📝 **NOTE:**   The MP Router must be disabled before you can change the PID format. If you do not explicitly disable the MP Router before performing this procedure, Advanced Web Tools disables the MP Router before applying the changes and then re-enables it afterward.

Setting the domain ID

A domain ID is assigned dynamically when a switch is enabled. However, you can manually set the domain ID to control the number or to resolve a domain ID conflict when merging fabrics. All the domain IDs in a fabric must be unique.

Displaying a list of domain IDs

Before assigning a domain ID to an MP Router, check the list of domain IDs already in the fabric so that you do not assign a duplicate.

1. Access the Switch Manager.
2. Click **Fabric** in the navigation bar (see Figure 5 on page 22).

   The fabric table lists all the domain IDs in the fabric.

Assigning a domain ID

To prevent a domain ID conflict, make sure all domain IDs are unique before connecting a switch to the fabric. You can also disable the switch until it is connected to the fabric and then re-enable the switch afterwards; unique domain IDs are automatically assigned.

The MP Router must be disabled before the domain ID is changed. If the MP Router is enabled, it is automatically disabled before the domain ID is changed and then automatically enabled afterwards.

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Switch Information** tab (see Figure 8).
4. Click **Change Domain Id** in the task bar.

   The Change Domain Id window opens.
5. Click **Fabric Assigned** to automatically assign a unique domain ID, or
   click **Custom** to manually assign a domain ID.
6. If you clicked Custom in step 5, enter a domain ID.

   The domain ID must be between 1 and 239 inclusive, and must be unique within the fabric.
7. Click **OK**.
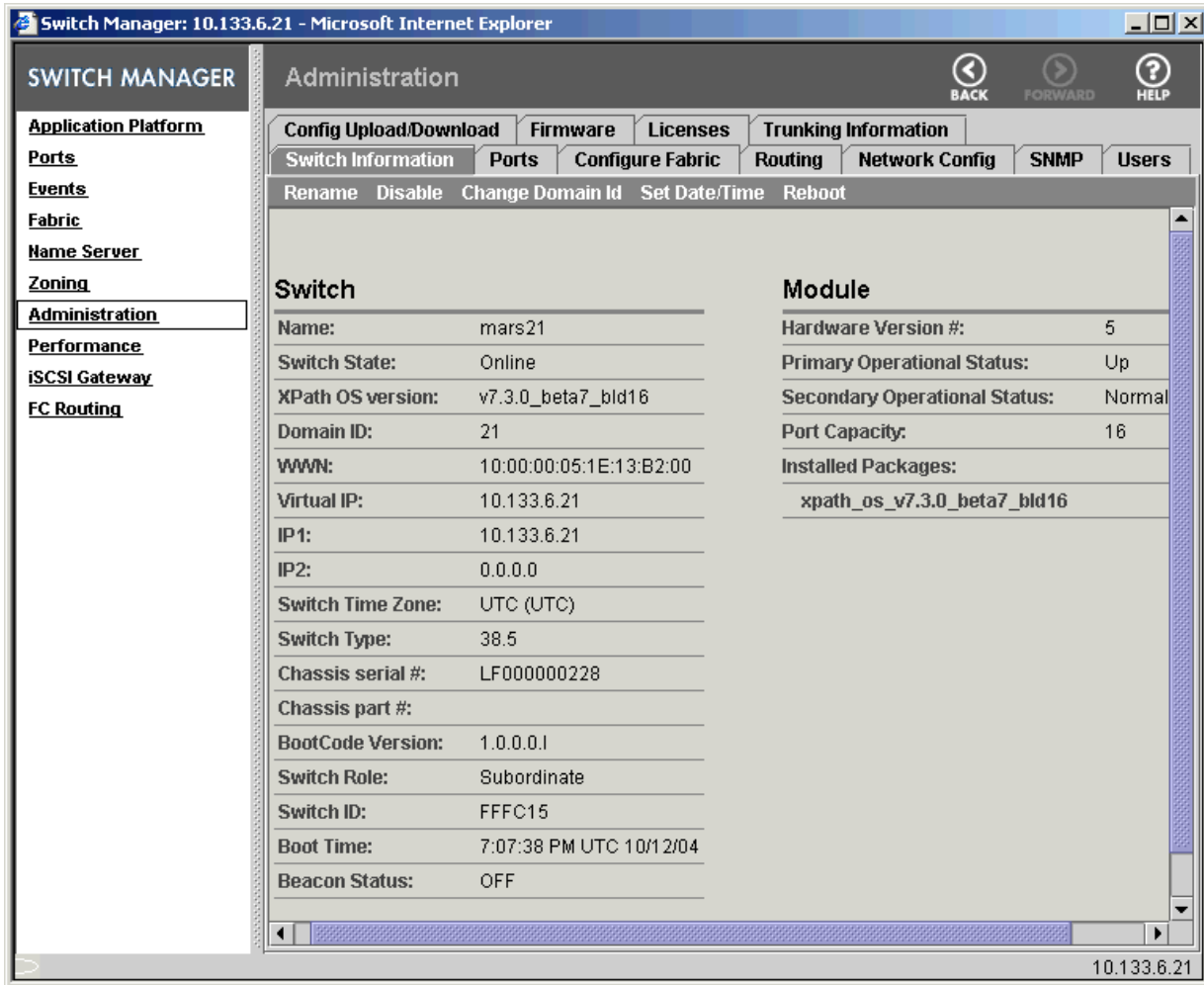
Figure 8 Administration page with the Switch Information tab selected

Verifying fabric connectivity

The MP Router forms a fabric when connected to a supported Fabric OS-based switch or another MP Router (if the ports on either side are enabled as E_Ports). See the installation guide for your switch for specific interswitch link (ISL) connection and cable management information.

1. Access the Switch Manager.
2. Click **Fabric** in the navigation bar.

   The Fabric page displays a summary of all the switches in the fabric, as shown in Figure 5 on page 22.

Verifying fabric-wide device connectivity

To view and verify that you have fabric-wide device connectivity, display the fabric-wide devices. The number of devices listed in the Name Server (NS) should reflect the number of devices that are connected.

1. Access the Switch Manager.
2. Click **Name Server** in the navigation bar.
3. Click the **All Devices** tab.

   This tab displays information about all the devices in the fabric (see Figure 9).

Figure 9 Name Server page with the All Devices tab selected

Viewing the device access map

If you enable a zone configuration, access between targets and initiators in the fabric is determined by that configuration. The Name Server page, Access Map tab displays all the targets and initiators and indicates which initiators can access which targets for the enabled zone configuration.

The target names and initiator names are hyperlinks that, when clicked, open a drill-down page for those items. A dot in the matrix indicates that an initiator can access the target.

1. Access the Switch Manager.
2. Click **Name Server** in the navigation bar.
3. Click the **Access Map** tab.

   This pane displays information about all the devices in the fabric (see Figure 10).
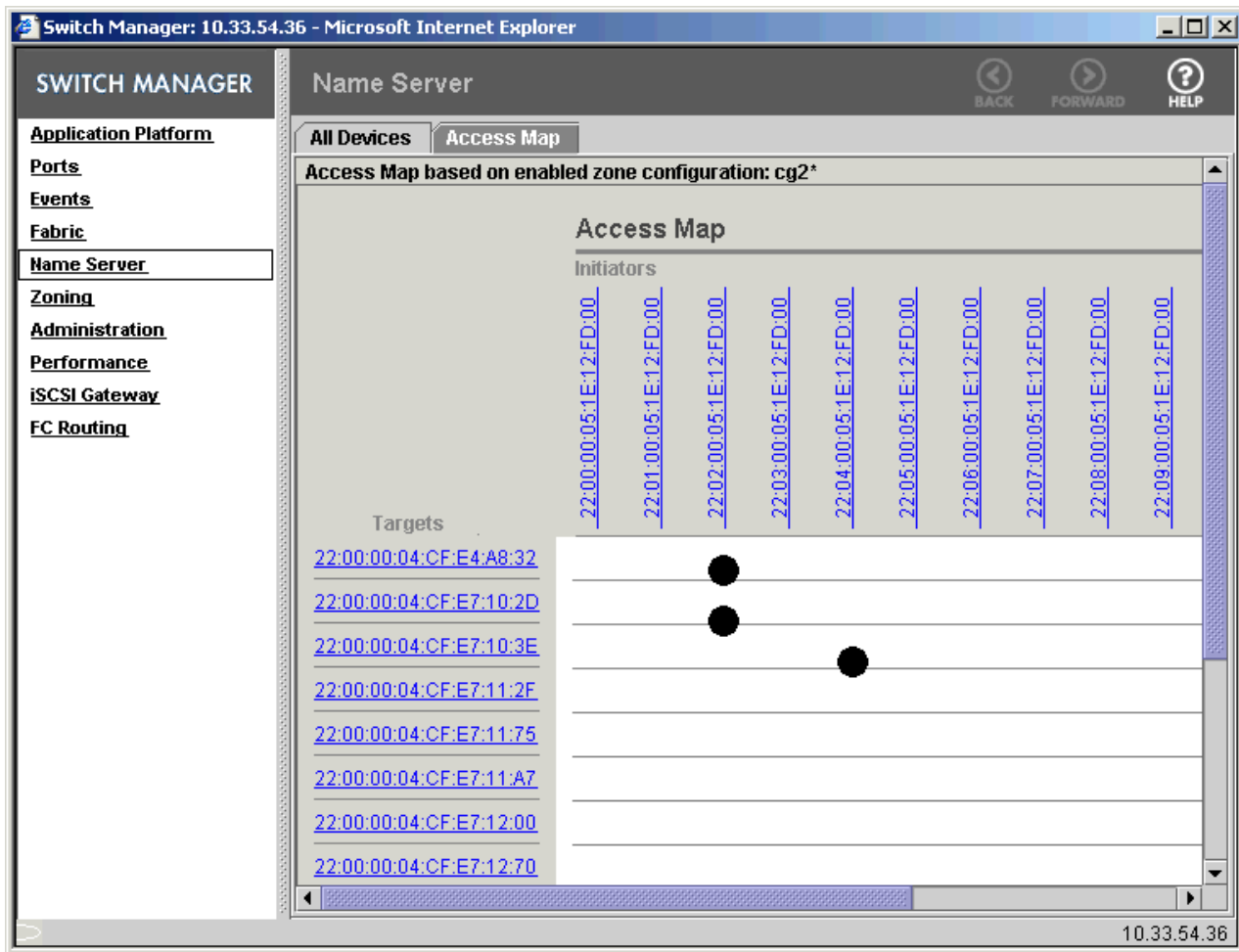
Figure 10 Name Server page with the Access Map tab selected

3 Managing the MP Router

This chapter provides procedures for managing the MP Router. It contains the following sections:

- Managing MP Routers with Advanced Web Tools, next
- Viewing switch information, page 31
- Opening a Telnet window, page 32
- Setting the switch date and time, page 32
- Configuring Ethernet management ports, page 33
- Verifying, installing, and removing licenses, page 34
- Managing user accounts, page 36
- Enabling and disabling an MP Router, page 37
- Renaming an MP Router, page 38
- Setting the domain ID, page 38
- Rebooting the MP Router, page 38
- Physically locating a switch using beaconing, page 39
- Updating the MP Router firmware, page 39
- Viewing SNMP information, page 41

Managing MP Routers with Advanced Web Tools

You can monitor and manage MP Routers through both the Switch Explorer and the Switch Manager. Most of the management tasks are performed through the Switch Manager, using the Application Platform page and the Administration page.

Click **Application Platform** in the Switch Manager navigation bar to access the Application Platform page. Figure 3 on page 16 shows the Application Platform page with the Summary tab selected. Click **Administration** in the Switch Manager navigation bar to access the Administration page. These pages, and the tasks you can perform from them, are described in more detail in the following sections.

Viewing switch information

You can view switch information from either the Switch Explorer or the Switch Manager.

Viewing switch information through the Switch Explorer

1. Select the switch or MP Router in the fabric tree.

   The Switch View displays a color-coded representation of the switch. The color of the Status, Fan, Temp, and Power buttons indicates the general status of these components. The Switch Information View displays general information about the switch (see Figure 2 on page 14).
2. Click the **Status** button to display the overall switch status.
3. Click the **Info** button to display general switch information.
4. Click the **Fan**, **Temp**, and **Power** buttons to display detailed state information about the fans, temperature sensors, and power supplies, respectively.

Viewing switch information through the Switch Manager

1. Click **Application Platform** in the navigation bar.
2. Click the **Summary** tab to display general information about the MP Router (see Figure 3 on page 16).
3. Click the **Details** tab to display information about the hardware components (see Figure 11 on page 32). To refresh the display for the temperature and fan status, click the corresponding **Refresh** button.
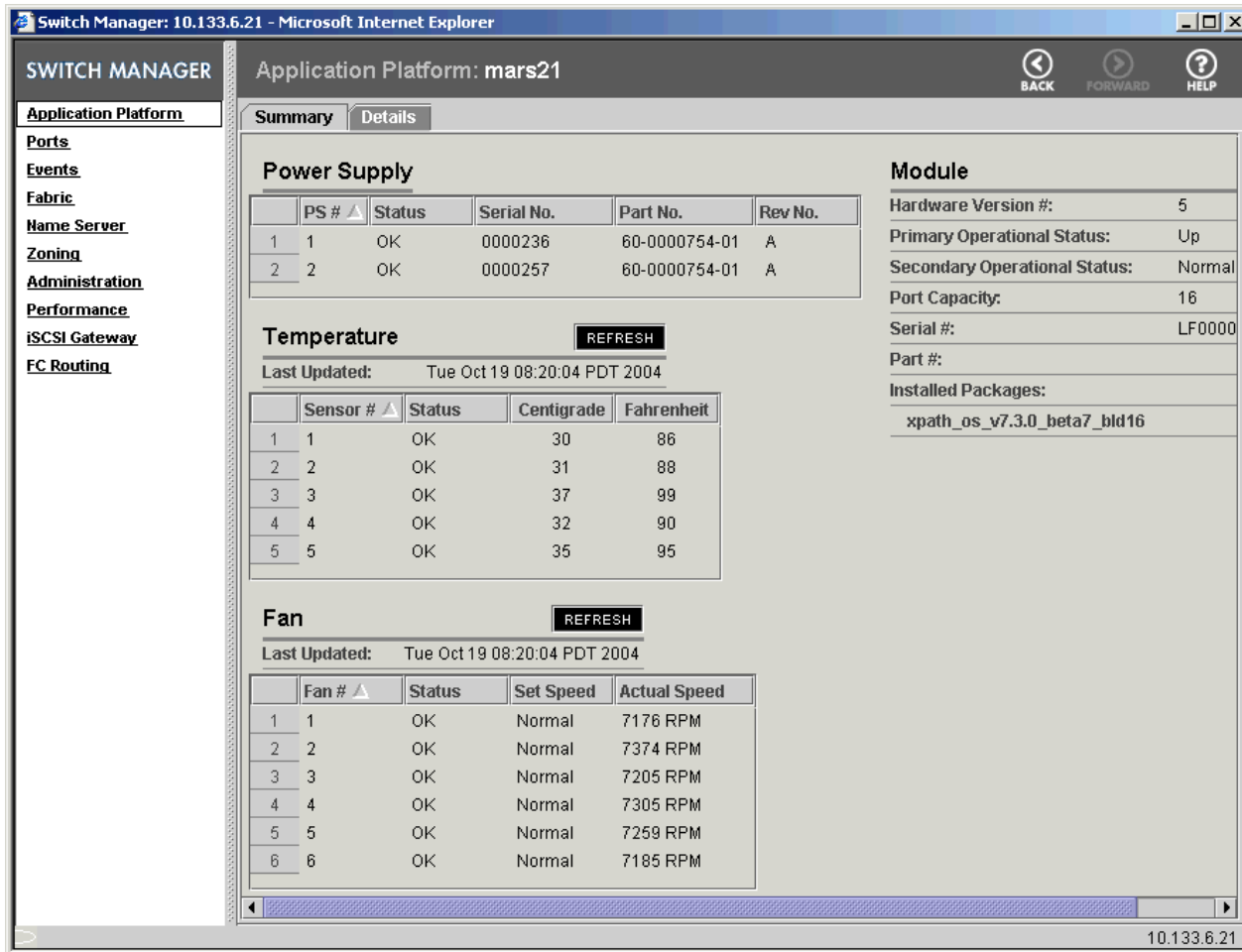
Figure 11 Application Platform page with Details tab selected

Opening a Telnet window

You can open a Telnet window to connect directly to the MP Router to perform any tasks that cannot be performed using the GUI. Use the following procedure to open a telnet window:

📝 **NOTE:** Telnet does not work in Mozilla due to technical limitations in Mozilla.

---

1. From the Switch Explorer, click the **Telnet** icon in the Switch View or from the Switch Manager click **Application Platform** in the navigation bar.
2. Click the **Summary** tab.
3. Click **Telnet** in the task bar.
   The Telnet window opens.

Setting the switch date and time

All switches maintain current date and time in nonvolatile memory. Date and time are used for logging events. Switch operation does not depend on the correct date and time; however, if they are incorrect the event log will have the incorrect dates and times.

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Switch Information** tab (see Figure 8 on page 28).
4. Click **Set Date/Time** in the task bar.
   The Set Switch Date/Time window opens.

5. Select the date from the drop-down calendar or manually enter the date in the format mm/dd/yyyy.
6. Enter the time in the format hh:mm.
7. Select **AM** or **PM**.
8. Select the continent or ocean that is closest to your location from the TimeZone Region drop-down list.
9. Select the country or city that has your time zone from the Location drop-down list.
10. Click **OK**.

Configuring Ethernet management ports

The MP Router provides two 10/100 Mbit/sec Ethernet ports capable of being configured as a single IP address or as two unique IP addresses.

If you configure the Ethernet ports with unique IP addresses, when the switch is joined to a fabric, the switch must have a virtual Ethernet IP identity for routing. If you change the IP address, the virtual IP address does not automatically change. You can handle this by setting a virtual management IP address for the switch.

The virtual management IP address is used as the single identity of the switch.

You must configure at least one of the Ethernet ports; this management IP address need not be the same as the virtual IP address. If management port 2 is not set, the virtual management IP address is the same as the management port 1 IP address.

You can launch Advanced Web Tools using any of the management or virtual management IP addresses.

Configuring IP and mask information

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Network Config** tab (see Figure 12).
4. Click **Edit**.
   The Edit Ethernet Management Ports dialog box opens.
5. Click the management ports you want to change (virtual management port, management port 1, and management port 2).
6. For each management port you are editing:
   a. Enter a valid IP address and subnet mask.
   b. Enter a valid gateway address (not applicable for the virtual management port).
   c. Select when the changes are to take effect (either immediately or after the next reboot) from the drop-down list.
7. Click **OK**.
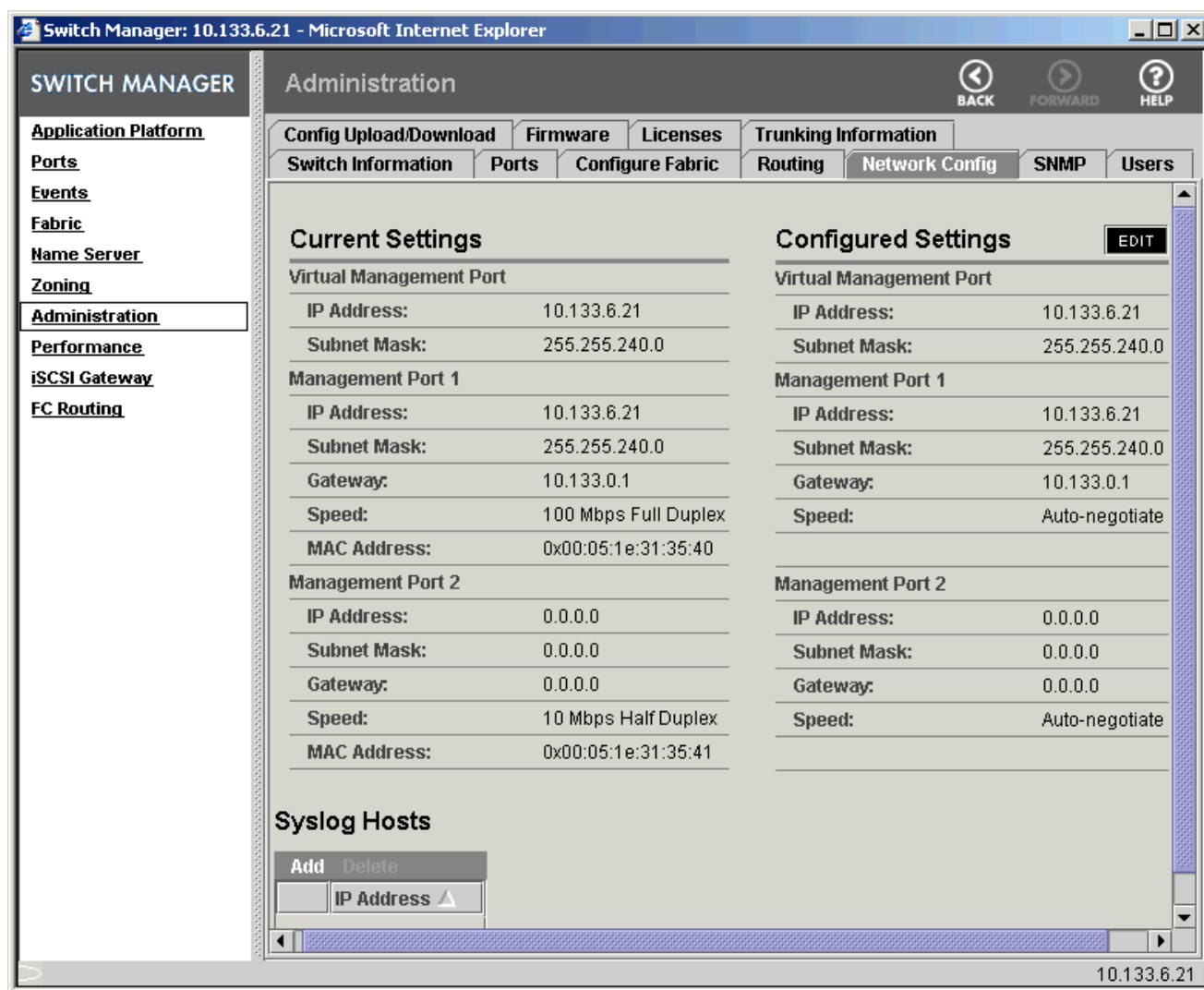
Figure 12 Administration page with the Network Config tab selected

Verifying, installing, and removing licenses

Some features of the MP Router and of the fabric to which it is connected are optional, licensed products. Without a license installed, these features do not function.

A license key is a string of approximately 16 uppercase and lowercase letters and numerals. Case is significant. The key is an encrypted form of the system WWN and the products licensed to run on the system.

The license key must be entered into the system exactly as issued. If entered incorrectly, the license might be accepted, but licensed products do not function. After entering the license, check for correct functioning. If no licensed products are displayed, the license is invalid.

After entering a license key, the licensed product is available immediately; the MP Router need not be rebooted.

Displaying licenses installed on the switch

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Licenses** tab.

A list of installed licenses and enabled features is displayed (see Figure 13 on page 35).

Adding a license to a switch

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Licenses** tab.
4. Click **Add** in the task bar.
5. Enter the license key.
6. Click **Add License**.

Removing a license from a switch

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Licenses** tab.
4. Select the license to remove.
5. Click **Remove** in the task bar.
6. Click **Yes** in the Confirmation window.
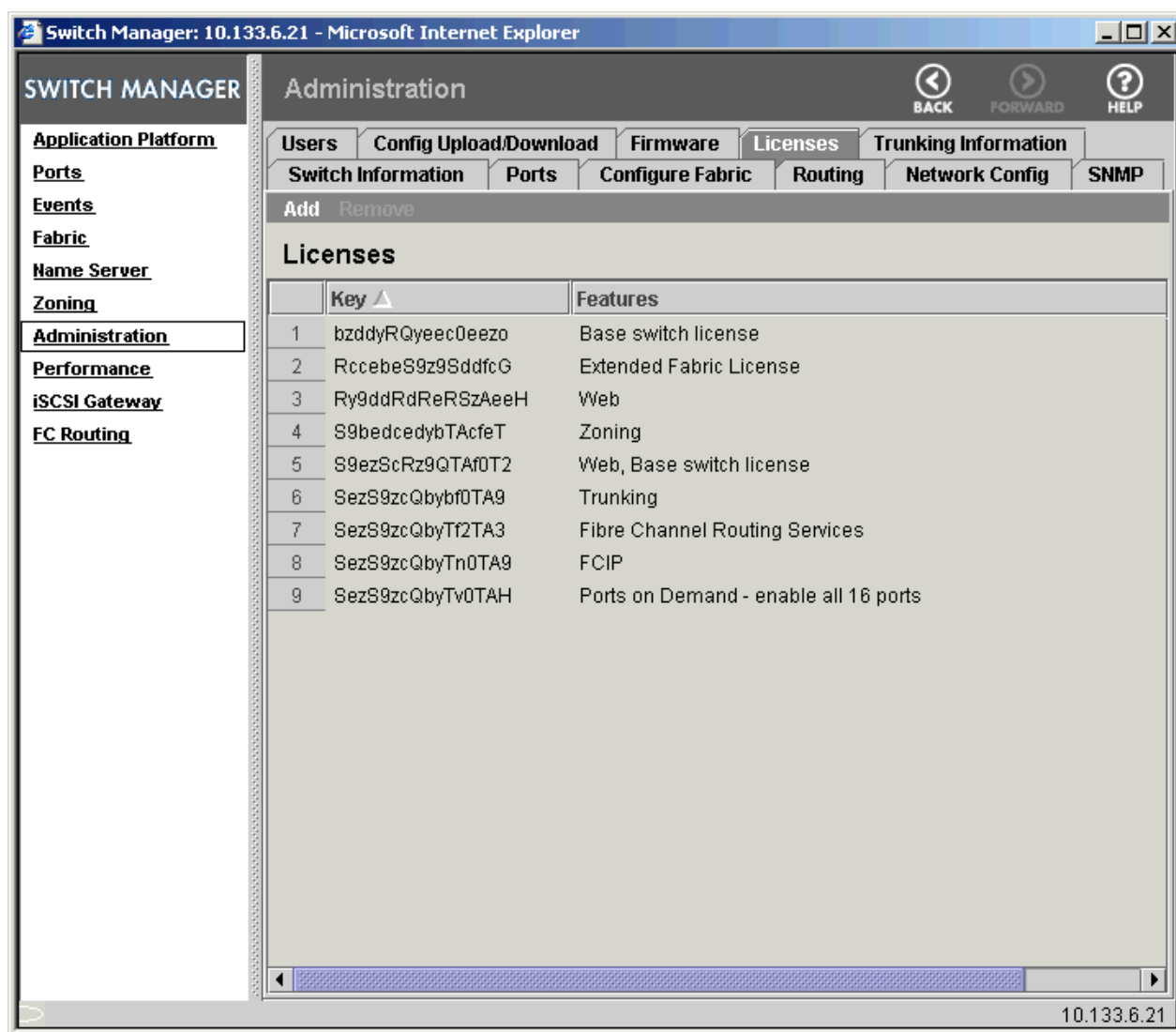
Figure 13 Administration page with the Licenses tab selected

Managing user accounts

Accounts are either in the admin group or the user group. Accounts belonging to the admin group can set the password to the default for all accounts belonging to the admin group or user group; but accounts belonging to the user group can change only the password for their own login.

For example, if you are logged in as an admin account `admin1`:

- You can change the password for the admin1 account.
- You can reset the passwords to the default for all other admin-level and user-level accounts.

However, if you are logged in as a user account `user1`:

- You can change the password only for the user1 account.

The Users tab on the Administration page displays a list of all the user accounts for the MP Router (see Figure 14 on page 37).

Adding a user

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Users** tab.
4. Click **Add User** in the task bar.
5. Enter the user name in the dialog box.
6. Select whether this user has user or admin privileges.
7. Click **OK**.

Deleting a user

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Users** tab.
4. Select the users to delete.

📝 **NOTE:** You cannot delete an account with the user names of `admin` or `user`.

---

5. Click **Delete User** in the task bar.
6. Click **Yes** in the confirmation window.

Changing password

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Users** tab.
4. Select your account.
5. Click **Change Your Password** in the task bar.
6. Enter your old password.
7. Enter the new password.
   The maximum length of a password is eight characters.
8. Re-enter the new password in the **Confirm New Password** box.
9. Click **OK**.

Resetting passwords to default values

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Users** tab.
4. Select the users whose passwords are to be reset.
5. Click **Reset Password** in the task bar.
6. Click **Yes** in the confirmation window.
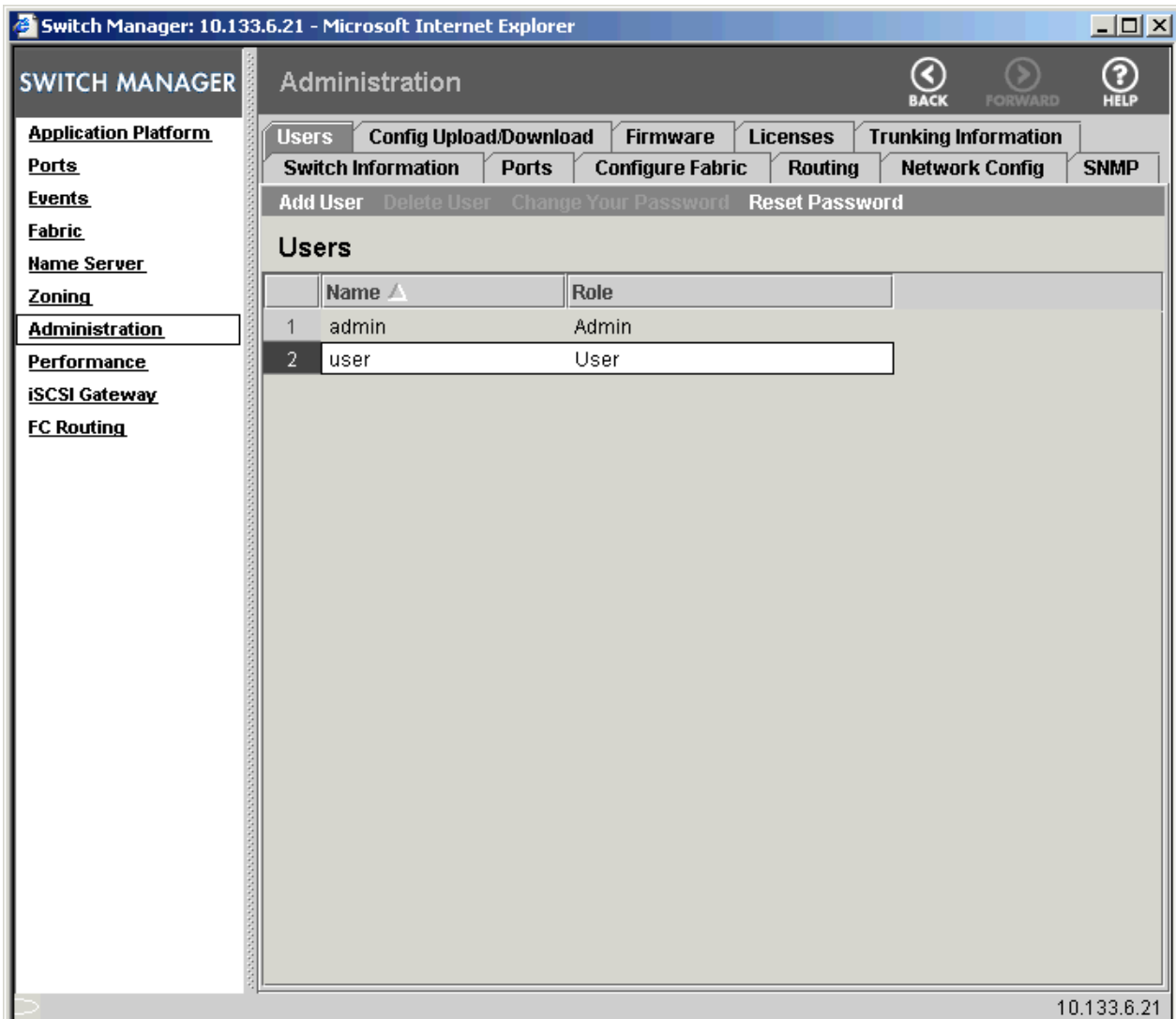
Figure 14 Administration page with the Users tab selected

Enabling and disabling an MP Router

This section describes how to enable and disable an MP Router.

Enabling an MP Router

When an MP Router boots, all Fibre Channel and Gigabit Ethernet (GigE) ports that passed the power-on self test (POST) and were enabled before the MP Router rebooted are enabled. If the MP Router was part of a fabric, it rejoins the fabric.

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Switch Information** tab (see Figure 8 on page 28).

4. Click **Enable** in the task bar.

   If Enable does not appear in the task bar, the switch is already enabled.

   The Enable Application Platform window opens.

5. Click **OK**.

Disabling an MP Router

When an MP Router is disabled, all Fibre Channel ports on it are taken offline. If the MP Router was part of a fabric, the fabric reconfigures.

Disabling an MP Router disconnects all currently connected devices and switches. No devices can connect to this MP Router until it is re-enabled.

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Switch Information** tab (see Figure 8 on page 28).
4. Click Disable in the task bar.

   If **Disable** does not appear in the task bar, the switch is already disabled.

   The Disable Application Platform window opens.

5. Click **OK** in the confirmation window.

Renaming an MP Router

You can customize the MP Router name. If you change the default name, be sure to choose a name that is unique and meaningful.

MP Router names have the following characteristics:

- They contain up to 19 characters.
- They begin with a letter or numeral.
- They consist of any combination of alphanumeric and underscore characters and spaces.

Use the following procedure to rename an MP Router:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Switch Information** tab (see Figure 8 on page 28).
4. Click **Rename** in the task bar.

   The Rename Application Platform window opens, displaying the current MP Router name.

5. Enter a new name and click **OK**.

Setting the domain ID

A domain ID is assigned dynamically when a switch is enabled. However, you can manually set the domain ID to control the number or to resolve a domain ID conflict when merging fabrics. See "Setting the domain ID" on page 26.

Rebooting the MP Router

When you reboot an MP Router, the Switch Manager loses connection to it until it finishes rebooting.

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Switch Information** tab (see Figure 8 on page 28).
4. Click **Reboot** in the task bar.

   The Reboot Switch window opens.

5. Click **Regular Reboot** to reboot the MP Router, or click **Fast Reboot** to reboot the MP Router and bypass the POST diagnostics.

6. Click **OK**.

Physically locating a switch using beaconing

Use the beaconing function to physically locate a switch in a fabric. The beaconing function helps you physically locate a switch by alternately blinking the system LED green and amber.

The Beacon button in the Switch Explorer indicates whether beaconing is on or off. The button displays a lighted beacon if beaconing is on.

Turning the beacon on

1. Select the switch from the fabric tree in the Switch Explorer.

   The selected switch appears in the Switch View.

2. Click the **Beacon** icon in the Switch View.

3. Click **Yes** to turn the beacon on.

4. Click **OK** to close the information window.

5. From Switch Manager, click **Application Platform** in the navigation bar.

6. Click the **Summary** tab.

7. Click **Turn Beacon On** in the task bar.

8. Click **Yes** to turn the beacon on.

9. Click **OK** to close the information window.

Turning the beacon off

1. From Switch Explorer, select the switch from the fabric tree.

   The selected switch appears in the Switch View.

2. Click the lighted **Beacon** icon in the Switch View.

3. Click **Yes** to turn the beacon off.

4. Click **OK** to close the information window.

5. From Switch Manager, click **Application Platform** in the navigation bar.

6. Click the **Summary** tab.

7. Click **Turn Beacon Off** in the task bar.

8. Click **Yes** to turn the beacon off.

9. Click **OK** to close the information window.

Updating the MP Router firmware

MP Router software is distributed in *packages*, which have both a *type* and a *version number*. The package name is built from the package type and the version number, for example, the package `xpath_os_7_1_0` consists of the package type, xpath_os, and the version number, 7_1_0.

One type of package is XPath OS itself. Other typical packages include application program packages. Bundling software in packages allows you to upgrade one type of software without affecting another. For example, you might upgrade an XPath OS version without affecting application packages.

MP Routers contain a single, shared file system. During package installation, the package file is uncompressed and copied to the file system, overwriting all files therein. Files from an older package are replaced by files in the newly installed package of the same type (for example, XPath OS).

The Firmware tab of the Administration page contains the procedures for downloading the firmware packages. Figure 15 shows the Administration page with the Firmware tab selected.
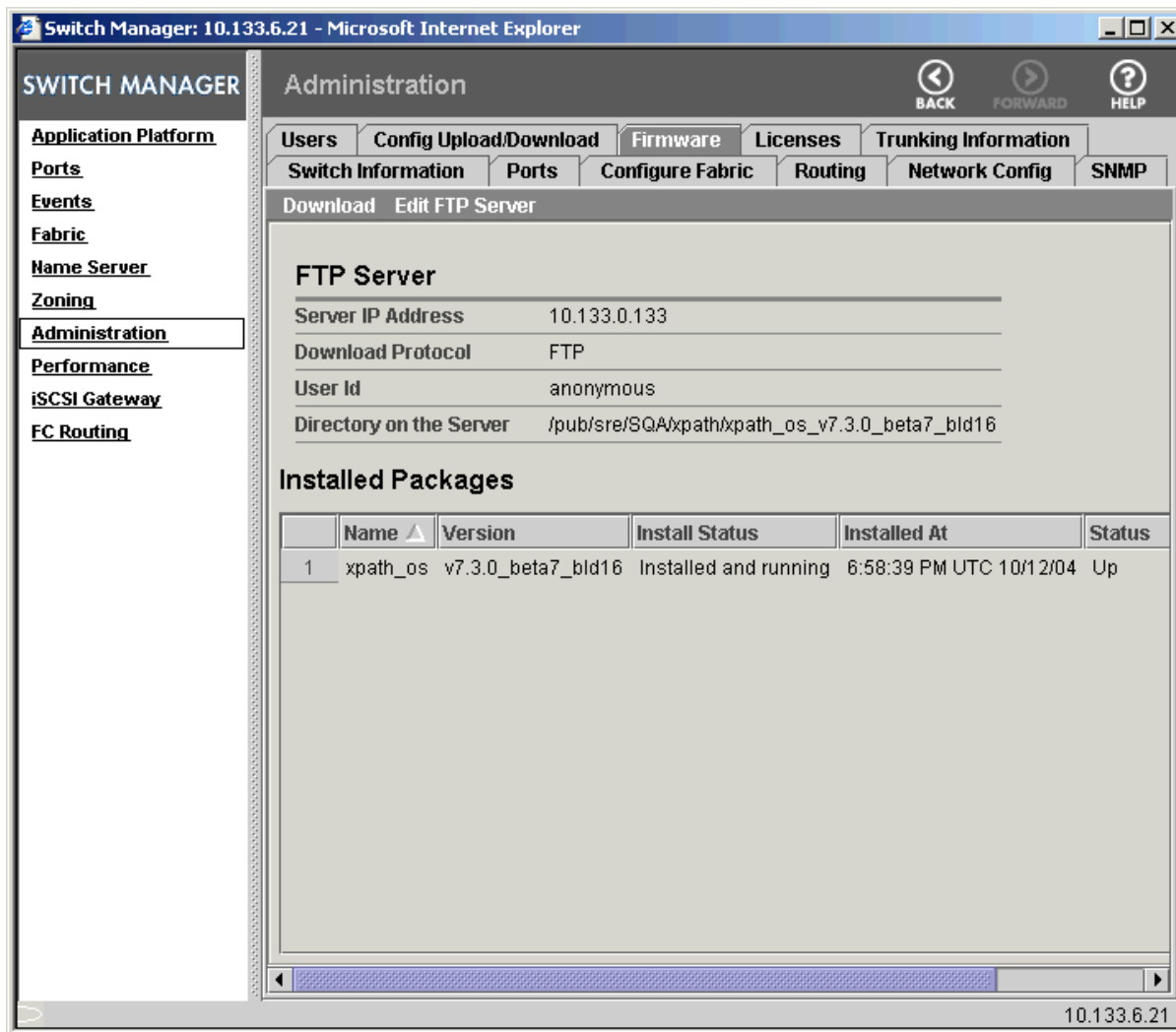
Figure 15 Administration page with Firmware tab selected

Displaying installed firmware versions

Use the following procedure to display firmware package information:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Firmware** tab (see Figure 15).

   The Installed Packages table lists information about the packages that are installed.

Installing a firmware package

Firmware packages are downloaded and installed from a remote FTP server in a single step. The FTP server is indicated on the Firmware pane in the FTP Server table.

📝 **NOTE:** Do not rename the firmware package file. One of the consistency checks performed during installation verifies that the actual file name and the original file name match.

Downloading and installing a firmware package to the MP Router

1. Access the Switch Manager.
2. Place the firmware package on the FTP server.
3. Click **Administration** in the navigation bar.

4. Click the **Firmware** tab (see Figure 15 on page 40).
5. Click **Download** in the task bar.
6. Optional: Click the **Edit Server** button to verify or change the server from which the package is to be downloaded.
7. Select the package to download from the File drop-down list.
8. Click **OK**.

   This process takes about fifteen minutes. Do not perform any other operation until the image download completes.

Upon completion, you must reboot the MP Router (see "Rebooting the MP Router" on page 38). The new configuration takes effect after the MP Router reboots.

Repeat this procedure if there are additional firmware packages.

📝 **NOTE:** Updating firmware does not change license keys, but new firmware might have new license requirements, for example, the new firmware might include a new feature requiring a new license. Check for changed license requirements when you update firmware.

Viewing SNMP information

This section explains how to view SNMP information and manage trap recipients. These procedures are performed from the SNMP tab of the Administration page, which is shown in Figure 16.

The SNMP pane displays the following SNMP agent system parameters, which correspond to variables in the MIB II system group:

- System Name corresponds to sysName.
- System Description corresponds to sysDesc.
- System Contact corresponds to sysContact.
- System Location corresponds to sysLocation.

For the Event Trap Level, when an event occurs, if its severity level is at or below the specified numeric value, the agent sends the associated trap to the configured recipients.
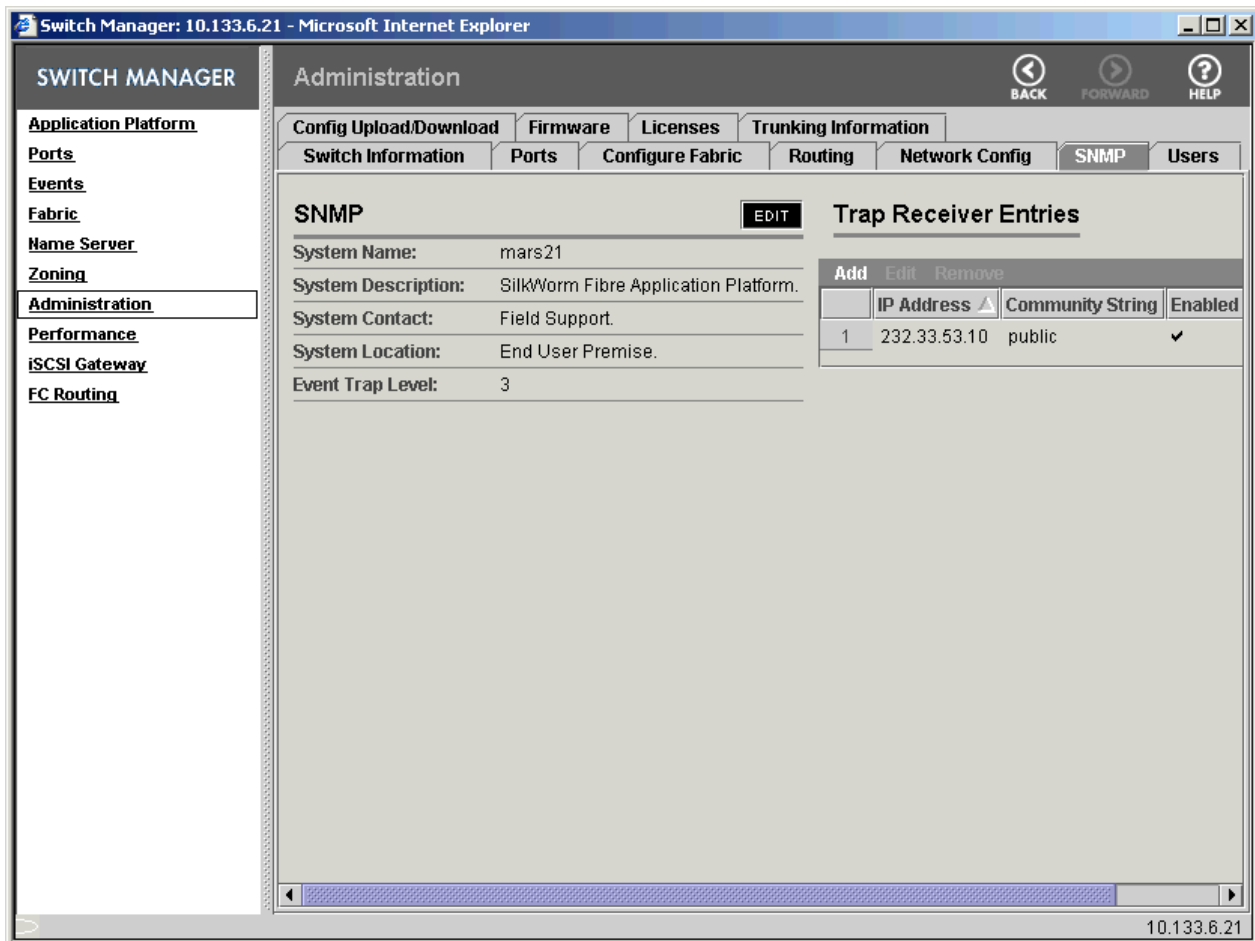
Figure 16 Administration page with SNMP tab selected

Configuring SNMP information

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **SNMP** tab.
4. Click the **Edit** button.
5. Enter the system name, description, contact, and location.
6. Enter the event trap level, which is an integer between 0 and 5, inclusive.
7. Click **OK**.

Adding a trap recipient

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **SNMP** tab.
4. Click **Add** in the Trap Receiver Entries task bar.
5. Enter the IP address and community string of the trap recipient.
6. Click **OK**.

Modifying a trap recipient

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **SNMP** tab.
4. Select the trap recipient in the Trap Receiver Entries table.
5. Click **Edit** in the Trap Receiver Entries task bar.
6. Enter the IP address and community string of the trap recipient.
7. Click **OK**.

Deleting a trap recipient

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **SNMP** tab.
4. Select the trap recipient in the Trap Receiver Entries table.
5. Click **Remove** in the Trap Receiver Entries task bar.
6. Click **Yes** in the confirmation window.

4 Managing ports

This chapter provides procedures for configuring and managing ports. It consists of the following sections:

- Managing ports with Advanced Web Tools, next
- Configuring a port, page 46
- Renaming a port, page 50
- Starting and stopping a port, page 51
- Enabling and disabling a port, page 52

Managing ports with Advanced Web Tools

You can monitor and manage ports through the Switch Manager. Click **Ports** in the navigation bar to access the Ports page. Figure 17 on page 46 shows the Ports page with the All Ports tab selected.

The Ports page displays the ports on the MP Router. You can view all the ports by clicking the All Ports tab, or you can view only ports of a certain type by clicking the Fibre Channel Ports, FCIP Ports, or iSCSI Ports tab.

For more detailed information on a specific port, click the port name to display a drill-down page for that port, as shown in Figure 4 on page 18. The name of the port is listed at the top of the page and is also indicated in the port diagram.

The port drill-down page has several tabs that you can select to display additional information about the port. Click the **General** tab to display port configuration and status information. Click the **SFP** tab to display information about the small-form-factor pluggable (SFP). Click the **Port Statistics** tab to display port counters.

You can perform port management tasks from either the Ports page or the port drill-down page. The Ports page allows you to configure multiple ports at the same time by selecting multiple ports and then clicking an action in the task bar.

NOTE: The color of the port icon in Advanced Web Tools does not indicate the port speed and does not change when you change port speed, unlike on the MP Router.
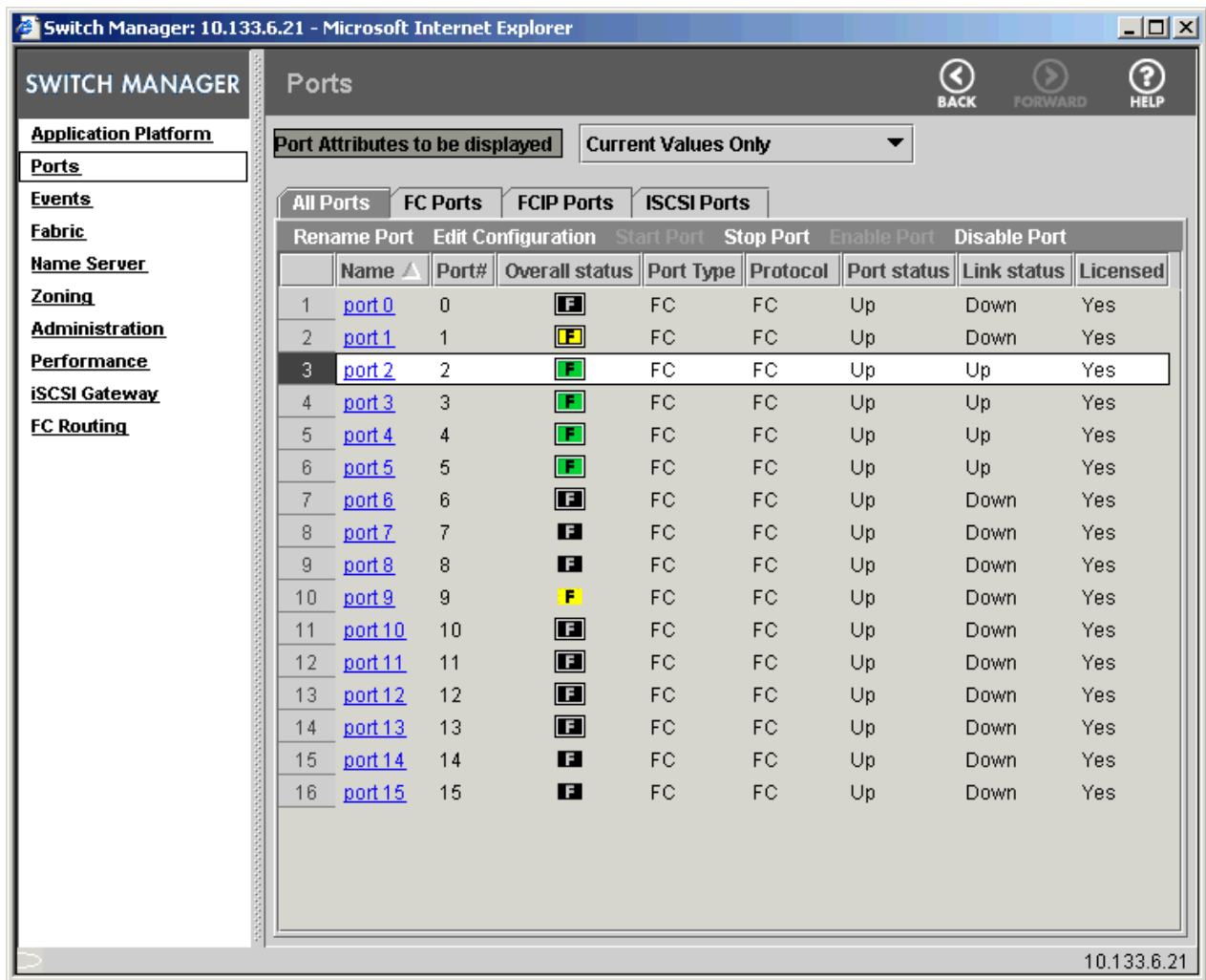
Figure 17 Port page with All Ports tab selected

Configuring a port

Configuring a port requires the port to be stopped first. If you do not explicitly stop the port before configuring it, it will be automatically stopped during the configuration process and then restarted when the configuration is complete.

You can configure the following ports:

- Fibre Channel U_Port
- Fibre Channel EX_Port
- Gigabit Ethernet (GigE) port for FCIP connectivity
- Gigabit Ethernet port with iSCSI

An EX_Port is a port on a Fibre Channel router that connects to an E_Port in an edge fabric. See "Using the FC-FC Routing service" on page 87, for more information.

A GigE port is used for sending and receiving FCIP network. See the *HP StorageWorks XPath OS 7.4.x command reference guide* for additional information about FCIP.

Use the following procedure to configure a port:

1. Access the Switch Manager for the switch on which the port resides.
2. Click **Ports** in the navigation bar.
3. Click the appropriate tab, depending on the type of port or click the **All Ports** tab to display all ports, regardless of type.

4. Highlight the port entry in the resulting table.

📝 **NOTE:** You can select more than one port to configure at a time, if you configure multiple ports to have the same values. The configuration is then changed for all the selected ports.

Clicking the port name displays a port drill-down page with additional information about the port; you do not need to open the drill-down page, however, to configure the port.

5. Click **Edit Configuration** in the task bar.

The Edit Port Configuration window opens (see Figure 18). The options in this window vary, depending on the licenses installed on the switch.

From here on, the procedure differs, depending on the type of port you are configuring:

- Fibre Channel port U_Port
- Fibre Channel port EX_Port
- Gigabit Ethernet port with FCIP
- Gigabit Ethernet port with iSCSI
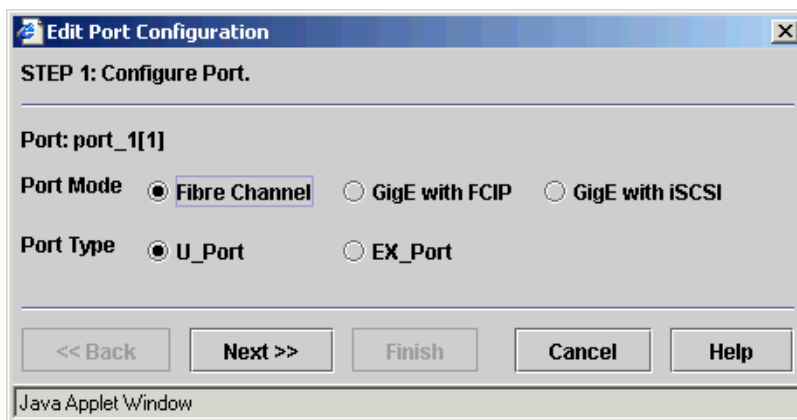
Figure 18 Edit Port Configuration window

Configuring a Fibre Channel U_Port

1. Select **Fibre Channel** for the port mode.

2. Select the port type: **U_Port**.

3. Click **Next**.

4. Select the port topology from the drop-down list: **Point to Point** or **Loop**.

In point-to-point mode (default), a port autodetects whether there is another switch on the other end of the connection (in such, case the port automatically becomes an E_Port) or whether there is a host or target on the other end (in such case, the port automatically becomes an F_Port).

In loop mode, the MP Router supports only one device in the loop.

5. Select the port speed from the drop-down list: **Auto** (for autonegotiate), **1 Gbps**, or **2 Gbps**.

6. Select the link cost:

- Click **Auto** to automatically set the link cost to the default link cost, which is based on port speed (for 1-Gbit/sec, the link cost is 1000; for 2-Gbit/sec, the link cost is 500).
- Click **Custom** to specify a static cost for the link, and enter the static link cost.

The cost of a link is used to determine the least-costly path for a frame from the source to the destination switch.

7. Select the maximum distance for the port-specific long-distance setting.

   Use the Max Distance setting to allocate enough full-size frame buffers on a particular port to support a long-distance link up to 300 km. This port-specific setting overrides any switch-wide BB_CREDIT setting.

   • **Normal (L0)**: Reconfigure the port to be a regular switch port. Switch-wide BB_CREDIT setting is used at this port.
   • **10 km (LE)**: This level supports distances up to 10 km at both 1-Gbit/sec and 2-Gbit/sec speeds.
   • **25 km (L0.5)**: This level supports distances up to 25 km at both 1-Gbit/sec and 2-Gbit/sec speeds.
   • **300 km (LS)**: This level supports distances up to 300 km at both 1-Gbit/sec and 2-Gbit/sec speeds.

📝 **NOTE:** If you are creating a long-distance ISL from the MP Router running XPath OS to a switch running Fabric OS 4.4.x or 3.2.x, you must set VC translation link initialization to 0 on the Fabric OS switch. VC translation link initialization is set to 1 by default in these Fabric OS versions, but it is not supported in XPath OS. For details on setting this option to 0, see Fabric OS documentation for the `portCfgLongDistance` command.

---

8. Select or clear the Allow as E Port checkbox, depending on whether or not the port is to function as an E_Port.

📝 **NOTE:** Selecting Allow as E Port results in fabric reconfiguration if the ports are enabled at both ends of the ISL.

---

9. Click **Finish**.

   If the port is not disabled, the Confirm Potential Disruption window opens, notifying you that the port is disabled before the configuration changes are applied.
10. Click **Yes** to disable the port and apply the configuration changes.
11. Click **Close** to close the Edit Port Configuration window.

   The edit configuration operation continues even if you close the window before the port is configured.

   After the configuration changes have been applied, the port is automatically enabled.

Configuring a Fibre Channel EX_Port

📝 **NOTE:** EX_Ports are used with the FC Routing feature.

---

1. Select **Fibre Channel** for the port mode.
2. Select the port type: **EX_Port**.

   An EX_Port is a port on a Fibre Channel router that connects to an E_Port in an edge fabric. See the Advanced Web Tools online help or the *HP StorageWorks XPath OS 7.4.x administrator guide* for more information about EX_Ports.
3. Click **Next**.
4. Select the port speed from the drop-down list: **Auto** (for autonegotiate), **1 Gbps**, or **2 Gbps**.

5. Select the maximum distance for the port-specific long-distance setting.

   Use the Max Distance setting to allocate enough full-size frame buffers on a particular port to support a long-distance link up to 300 km. This port-specific setting overrides any switch-wide BB_CREDIT setting.

   - **Normal (L0)**: Reconfigure the port to be a regular switch port. Switch-wide BB_CREDIT setting will be used at this port.
   - **10 km (LE)**: This level supports distances up to 10 km at both 1-Gbit/sec and 2-Gbit/sec speeds.
   - **25 km (L0.5)**: This level supports distances up to 25 km at both 1-Gbit/sec and 2-Gbit/sec speeds.
   - **300 km (LS)**: This level supports distances up to 300 km at both 1-Gbit/sec and 2-Gbit/sec speeds.

📝 **NOTE:** If you are creating a long-distance ISL from the MP Router running XPath OS to a switch running Fabric OS 4.4.x or 3.2.x, you must set VC translation link initialization to 0 on the Fabric OS switch. VC translation link initialization is set to 1 by default in these Fabric OS versions, but it is not supported in XPath OS. For details on setting this option to 0, see Fabric OS documentation for the `portCfgLongDistance` command.

6. Click **Next**.
7. Enter the fabric ID.

   This is the ID of the edge fabric that connects to the EX_Port. EX_Ports connected to the same edge fabric must have the same fabric ID. Note that this does not require any switch in the edge fabric to be configured with a fabric ID.

8. Select the interoperability mode: Brocade Native mode, McDATA Fabric mode, or **Open** (open fabric) mode.
9. Click **Finish**.

   If the port is not stopped, the Confirm Potential Disruption window opens, notifying you that the port is stopped before the configuration changes are applied.

10. Click **Yes** to disable the port and apply the configuration changes.
11. Click **Close** to close the Edit Port Configuration window.

    The edit configuration operation continues even if you close the window before the port is configured.

    After the configuration changes have been applied, the port is automatically restarted.

Configuring a Gigabit Ethernet port with FCIP

📝 **NOTE:** The FCIP feature is available only when a license for this feature is installed.

1. Select **GigE with FCIP** for the port mode and then click **Next**.
2. Enter values for the IP address, subnet mask, and gateway, and then click **Next**.
3. Select the link cost:
   - Click **Dynamic Link Cost** to automatically set the link cost based on port speed (for a 1-Gbit/sec ISL, the link cost is 1000; for a 2-Gbit/sec ISL the link cost is 500).
   - Click **Custom Link Cost** to specify a static cost for the link. Enter the static link cost in the **Custom Link Cost** box.

   The cost of a link is used to determine the least-costly path for a frame from the source to the destination switch.

4. Specify the FCIP values. Select from the following:
   - **Enable FCIP Tunneling**. Select this option to enable the Fibre Channel over IP ISL. FCIP tunneling allows the transparent interconnection of geographically distributed Storage Area Network (SAN) islands through an IP-based network. If the tunnel is not enabled, IP-level debugging can still be performed. See the *HP StorageWorks XPath OS 7.4.x command reference guide* for more information about FCIP Tunneling.

- **Restrict connections to switch with WWN**. If you select this option, the switch accepts only the incoming FCIP tunnel with the configured WWN; it also initiates a tunnel only to the desired switch. If you do not select this option, the switch accepts FCIP connections from any other switch.
- Click one of the following:
  - **Listen for tunnel connections**. If you select this option, the local switch listens for incoming connections for FCIP tunnels, but does not initiate tunnel establishment.
  - **Initiate tunnel connection**. If you select this option, the local switch sets up a TCP connection for the FCIP tunnel to the remote switch. You must also type the IP address of the remote port.

5. Click **Finish**.

   If the port is not stopped, the Confirm Potential Disruption window opens, notifying you that the port is stopped before the configuration changes are applied.

6. Click **Yes** to stop the port and apply the configuration changes.

7. Click **Close** to close the Edit Port Configuration window.

   The edit configuration operation continues even if you close the window before the port is configured.

   After the configuration changes have been applied, the port is automatically started.

> **NOTE:**   To establish a Fibre Channel over IP ISL between two MP Routers, you must configure the ports on both the local and remote MP Routers. At least one of the ports must be configured for listening *and* initiating tunnel connections.

Configuring a Gigabit Ethernet port with iSCSI

1. Select **GigE with iSCSI** for the port mode and then click **Next**.
2. Enter values for the IP address, subnet mask, and gateway.
3. Click **Finish**.

   If the port is not stopped, the Confirm Potential Disruption window opens, notifying you that the port is stopped before the configuration changes are applied.

4. Click **Yes** to disable the port and apply the configuration changes.
5. Click **Close** to close the Edit Port Configuration window.

   The edit configuration operation continues even if you close the window before the port is configured.

   After the configuration changes have been applied, the port is automatically started.

Renaming a port

Port names have the following characteristics:

- They must consist of at least 1 and not more than 32 characters.
- They can consist of any combination of printable characters or white spaces, excluding the following:
  - Comma (,)
  - Semicolon (;)
  - Ampersand (&)
  - At sign (@)
  - Percent sign (%)
  - Slash (/)
  - Tab

The default port names are `port num`, where *num* is an integer from 0 to 15, for example, port 0, port 1, port 2.

> **NOTE:**   Port names are not required to be unique. If you want port names to be unique, it is up to you to check; Advanced Web Tools does not enforce uniqueness.

Use the following procedure to rename a port:

1. Access the Switch Manager for the switch on which the port resides.
2. Click **Ports** in the navigation bar.
3. Click the appropriate tab, depending on the type of port.

   The All Ports tab displays all the ports, regardless of type.
4. Highlight the port entry in the resulting table.

   Clicking the port name displays a port drill-down page with additional information about the port; you do not need to open the drill-down page, however, to rename the port.
5. From the Ports page, click **Rename Port** in the task bar.
6. From the port drill-down page, click **Rename** in the task bar.

   The Rename Switch Port window opens.
7. Enter a new port name.
8. Click **OK**.

Starting and stopping a port

This section describes how to start and stop a port. You can select multiple ports and start or stop all of them in one operation.

Starting a port

Starting a port makes the port available and starts the port process that handles communication with the host. This is different from enabling a port, which enables the port laser.

Use the following procedure to start a port:

1. Access the Switch Manager for the switch on which the port resides.
2. Click **Ports** in the navigation bar.
3. Click the appropriate tab, depending on the type of port.

   The All Ports tab displays all the ports, regardless of type.
4. Highlight the port entry in the resulting table.

   Clicking the port name displays a port drill-down page with additional information about the port; you do not need to open the drill-down page, however, to start the port.
5. Click **Start Port** in the task bar.

   The Start Port window opens.
6. Click **OK**.

   The start operation begins.
7. Click **Close** to close the Start Port window.

   The start operation continues even if you close the window before the port is started.

   When the port is started, Port Status is `Up` and Port Admin Status (in the port drill-down page) is `Started`.

Stopping a port

Stopping a port stops the process running on the port. This is different from disabling a port, which disables the port laser.

Disable the port when you want to quickly stop the laser on the port, for example, when troubleshooting a connected device. Stop the port when you want to stop the code to a port for more involved troubleshooting or as part of reconfiguring the port to Fibre Channel or IP.

Stopping a port disconnects any devices or switches connected to the port. No devices or switches can connect to the port until the port is restarted.

Use the following procedure to stop a port:

1. Access the Switch Manager for the switch on which the port resides.
2. Click **Ports** in the navigation bar.

3. Click the appropriate tab, depending on the type of port.

 The All Ports tab displays all the ports, regardless of type.

4. Highlight the port entry in the table.

 Clicking the port name displays a port drill-down page with additional information about the port; you do not need to open the drill-down page, however, to stop the port.

5. Click **Stop Port** in the task bar.

 The Stop Port window opens.

6. Click **OK**.

 The stop operation begins.

7. Click **Close** to close the Stop Port window.

 The stop operation continues even if you close the window before the port is stopped.

 When the port is stopped, Port Status is Down. The port icon color is gray.

Enabling and disabling a port

This section describes how to enable and disable a port. You can select multiple ports and enable or disable all of them in one operation.

Enabling a port

Enabling a port enables the port laser. This is different from starting a port, which starts the port process that handles communication with the host.

When a port is enabled and is connected to one or more devices, these devices become available to the fabric. Use the following procedure to enable a port:

1. Access the Switch Manager for the switch on which the port resides.
2. Click **Ports** in the navigation bar.
3. Click the appropriate tab, depending on the type of port.

 The All Ports tab displays all the ports, regardless of type.

4. Highlight the port entry in the resulting table.

 Clicking the port name displays a port drill-down page with additional information about the port; you do not need to open the drill-down page, however, to start the port.

5. Click **Enable Port** in the task bar.

 The Enable Port window opens.

6. Click **OK**.

 The enable operation begins.

7. Click **Close** to close the Enable Port window.

 The enable operation continues even if you close the window before the port is started. When the port is enabled, Link Status is Enabled.

Disabling a port

Disabling a port disables the port laser. This is different from stopping the port, which stops the process running on the port.

Disable the port when you want to quickly stop the laser on the port, for example, when troubleshooting a connected device or switch. Stop the port when you want to stop the code to a port for more involved troubleshooting or as part of reconfiguring the port to Fibre Channel or IP.

If you disable a port that is connected to another switch, the fabric might reconfigure. If the port is connected to one or more devices, these devices are no longer available to the fabric, and the fabric reconfigures.

Use the following procedure to disable a port:

1. Access the Switch Manager for the switch on which the port resides.
2. Click **Ports** in the navigation bar.

3. Click the appropriate tab, depending on the type of port.

   The All Ports tab displays all the ports, regardless of type.

4. Highlight the port entry in the resulting table.

   Clicking the port name displays a port drill-down page with additional information about the port; you do not need to open the drill-down page, however, to disable the port.

5. Click **Disable Port** in the task bar.

   The Disable Port window opens.

6. Click **OK**.

   The disable operation begins.

7. Click **Close** to close the Disable Port window.

   The disable operation continues even if you close the window before the port is disabled.

   When the port is disabled, Link Status is Disabled and the port icon color is yellow (unless the port is stopped, in which case it is gray).

5 Managing zoning

This chapter briefly describes zoning and provides the procedures for managing zoning using Advanced Web Tools. It contains the following sections:

- Introduction to Zoning, next
- Managing zoning with Advanced Web Tools, page 57
- Configuring zoning, page 58
- Managing zone aliases, page 58
- Managing zones, page 61
- Managing zone configurations, page 65
- Configuring zone server attributes, page 69
- Saving zone information, page 69
- Deleting all zone information, page 69

Introduction to Zoning

HP Advanced Zoning is an optional, licensed feature that allows partitioning of a SAN into logical groupings of devices that have access to each other. These logical groupings are called *zones*. Zoning allows devices in a fabric to see some devices and not others. Using zoning, administrators can control access to devices. For example, you can partition the SAN into two zones, *winzone* and *unixzone*, so that the Windows servers and storage do not interact with UNIX® servers and storage. See "Verifying, installing, and removing licenses" on page 34 for information on adding a zoning license.

Zoning terminology

This chapter uses the following terminology to describe zoning:

zone	A set of devices or ports that can communicate only with other devices or ports within the set.
alias	A logical group of ports or WWNs. An alias is a way of representing one or more ports or devices by a more familiar name.
	Specifying groups of ports or devices as an alias makes zone configuration easier, by enabling you to configure zones using an alias rather than a long string of individual members. For example, you might assign all the WWNs of all the disks in a particular JBOD to the alias myJBOD. Then all of those devices can be added easily to any zone by adding the myJBOD alias to that zone.
zone member	An alias; port, domain ID and port pair; port WWN or node WWN that is part of a zone.
configuration	A specified set of zones. A fabric can store any number of zone configurations, but only one configuration is active at a time.
defined zone configuration	The set of all zone configurations defined in the fabric.
effective zone configuration	The currently enabled zone configuration (also known as the *active zone configuration*). Only one configuration can be enabled at a time. If no configuration is enabled, no zones are enforced and all devices can see each other. You cannot modify the effective configuration.

Zoning and MP Routers

Any device or zone member connected to the fabric can be included in one or more zones. Zone members within a zone can communicate only with other zone members in the same zone.

After zoning is enabled, if a device is not explicitly defined in a zone, that device is isolated and is inaccessible to other devices in the fabric.

Zone members are grouped into zones, and zones are grouped into a *zone configuration*. Zones can overlap; that is, a zone member can belong to more than one zone, and a fabric can have multiple zones. You can create multiple zone configurations, but only one configuration can be enabled in the fabric at a time.

Figure 19 shows a sample zone configuration with the following characteristics:

- Loop1 is not a member of any zone and is therefore inaccessible to other devices in the fabric.
- Loop2 is a member of both the Red Zone and the Green Zone. Both Server1 and Server3 can access Loop2, but Server1 and Server3 cannot access each other.
- Server2 cannot access Loop2 or either of Server1 or Server3. Server2 can access the RAID device.
- The RAID device is a member of both the Blue Zone and the Green Zone. The RAID device can be accessed by Server2 and Server3, but cannot be accessed by Server1.
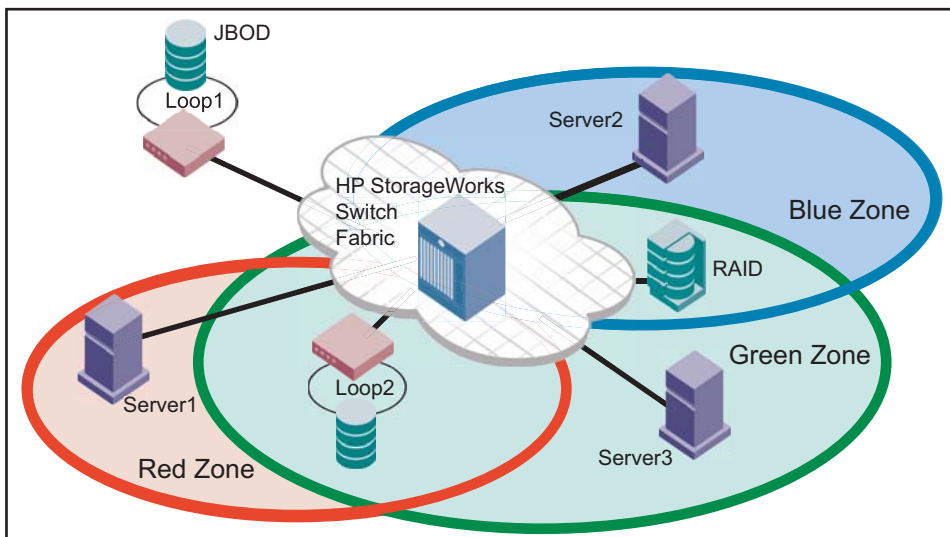
Figure 19 Sample zone configuration

A zone member can be specified using a domain, port pair, a node WWN, or a port WWN.

NOTE: Use port WWNs for Fibre Channel-attached nodes with Fibre Channel router LSAN zones.

Zoning enforcement

Two basic zoning enforcement mechanisms are used: one is called *software zoning* or *soft zoning* and the other is called *hardware zoning* or *hard zoning*.

HP Zoning software limits access to data by segmenting a fabric into virtual private SANs. Soft zoning prevents hosts from discovering unauthorized target devices, while hard zoning prevents a host from ever accessing a device it is not authorized to access.

The MP Router supports both soft and hard zoning, although only one is functional at a time. The Zone Server distributes the soft zoning information to the Name Server and the allowed S_ID/D_ID pairs to the appropriate ports for hard zoning. If the number of S_ID/D_ID pairs in a configuration is more than 1000, hard zoning switches over to soft zoning. XPath OS hard zoning can coexist with other implementations of hard zoning.

Soft zoning

In soft zoning, the Name Server, getting its information from the Zone Server, limits the targets returned to a Fibre Channel initiator to only those to which the Fibre Channel initiator can communicate, as specified by the zoning configuration. This is the method required by the Fibre Channel standards FC-SW-2, FC-GS-3, and FC-GS-4. If the Fibre Channel host bus adapters (HBAs) are standards-compliant, this method is reliable.

With soft zoning, an initiator that is a member of a zone has access only to the names and addresses of other members of the zone, and so cannot address frames to devices outside the zone.

It is important to note that software-enforced zoning does not prohibit access to the device. If an initiator has knowledge of the network address of a target device, it does not need to query the Name Server to access it, which could lead to undesired access to a target device by unauthorized hosts.

XPath OS implementation of soft zoning follows industry standards and offers compatibility with Fibre Channel switch zoning implementations.

Hard zoning

Hard zoning means that each frame is checked by hardware before it is delivered to a zone member and discarded if there is a zone mismatch.

Hard zoning enforcement must be used in those situations in which the HBAs are not standards-compliant, for example, when the hardware predates the standards. If security is a priority, HP recommends the use of hard zoning.

In XPath OS hard zoning, the frame source and destination addresses are compared to allowed addresses at the MP Router ingress F_Port (for devices directly attached to the MP Router) or at an egress F_Port (for devices directly attached to a non-HP switch). For additional information about hard zoning enforcement, see the *HP StorageWorks XPath OS 7.4.x administrator guide*.

Managing zoning with Advanced Web Tools

You can monitor and manage zoning through the Switch Manager. Click **Zoning** in the navigation bar to access the Zoning page. Figure 20 shows the Zoning page with the Zone Server tab selected.

If "Zoning" is missing from the navigation bar, this means that the zoning license is not activated. See "Verifying, installing, and removing licenses" on page 34 for instructions on installing a license.

📝 **NOTE:**   You cannot manage QuickLoop and Fabric Assist zones through Advanced Web Tools. Use the CLI to create, delete, and manage these types of zones. You can, however, use Advanced Web Tools to view these zones.
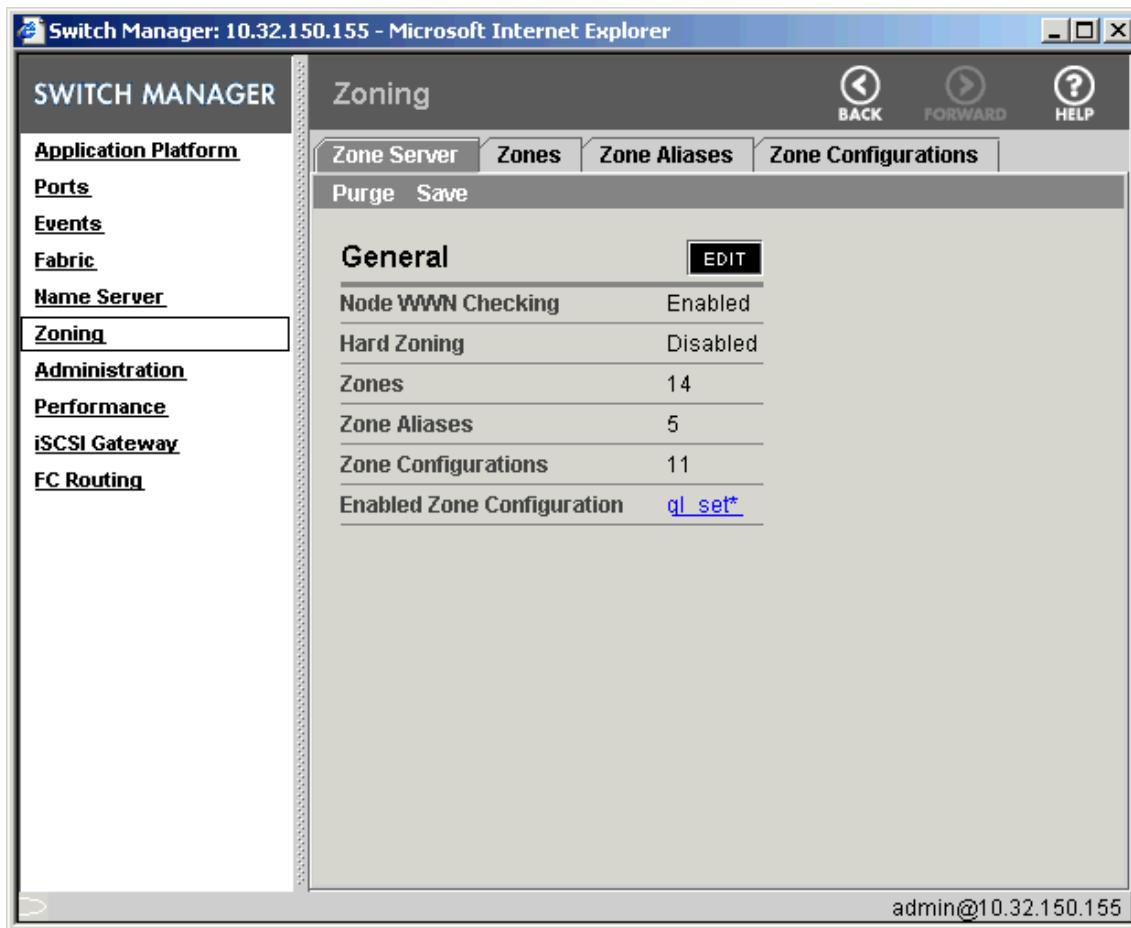
Figure 20 Zoning page with Zone Server tab selected

Configuring zoning

The MP Router can be included in zones using either domain, port or WWN naming, and both Fabric OS switches and XPath OS MP Routers enforce hard zoning on both WWN and domain, port zone object naming. However, note that if a zone configuration on one switch uses WWN naming and an identical zone configuration on another switch uses domain, port naming, the configurations do not merge, and the fabric segments.

1. Determine the zoning schemes you will use in the fabric.
2. Create zone aliases (see "Creating a zone alias" on page 59).
3. Create zones (see "Creating a zone" on page 62).
4. Create zone configurations (see "Creating a zone configuration" on page 66).
5. Enable a zone configuration (see "Enabling a zone configuration" on page 68).
6. Save the zone configuration (see "Saving zone information" on page 69).

The following sections provide procedures for managing zones, zone aliases, zone configurations, and zone server information.

Managing zone aliases

The Zone Aliases tab in the Zoning page displays a list of the zone aliases in the fabric and provides tasks for managing those zone aliases (see Figure 21). From this tab, you can create, rename, delete, clone, and save zone aliases. The procedures for these tasks are described next.

Unlike zones, zone aliases are never part of the effective zone configuration; when you enable a zone configuration, any zone aliases in the member zones are automatically expanded. Because of this, you can rename, delete, and modify zone aliases, even if they have been used to create zones that are members of the effective zone configuration.
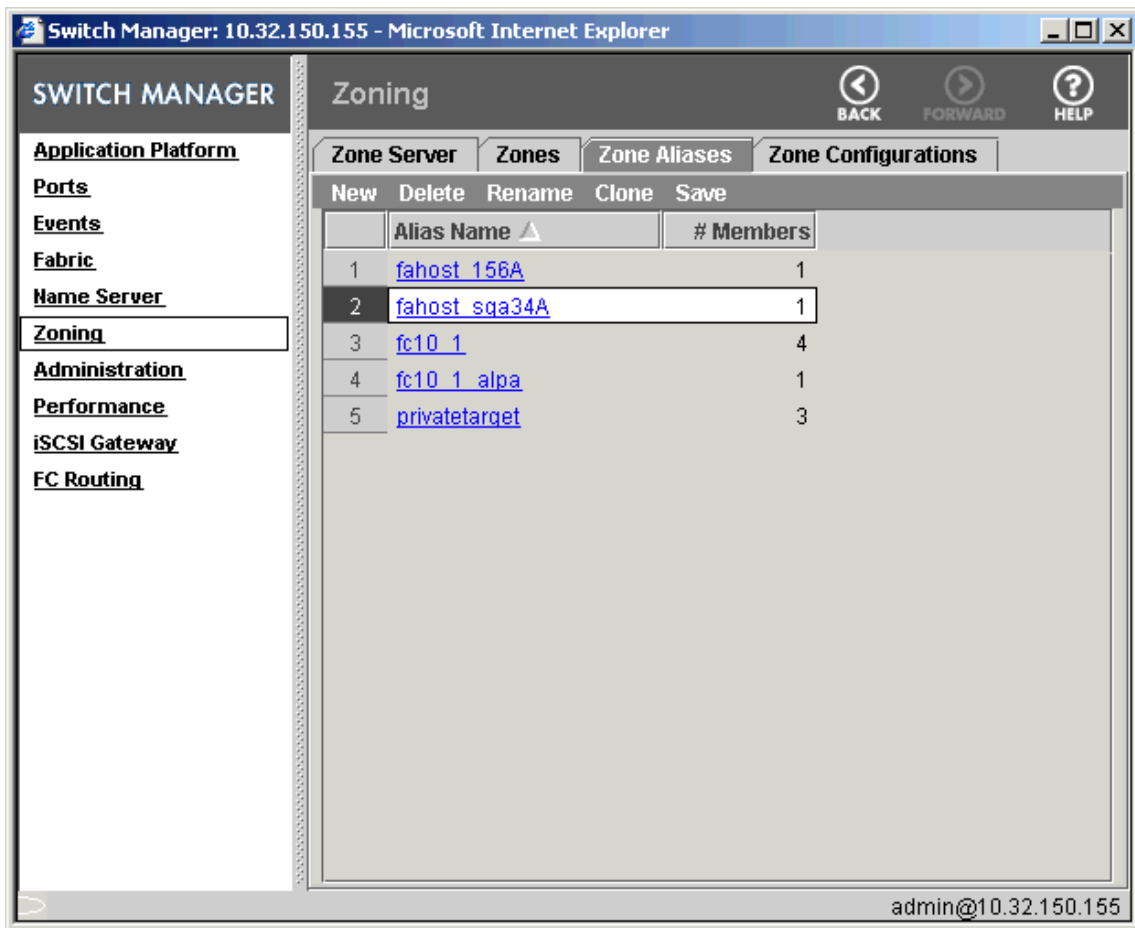
Figure 21 Zoning page with Zone Aliases tab selected

Creating a zone alias

An alias is a logical group of ports or WWNs. Specifying groups of ports or devices as an alias makes zone configuration easier by enabling you to configure zones using an alias rather than a long string of individual members. Use the following procedure to create a zone alias:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Aliases** tab.
3. Click **New** in the task bar.

   The New Zone Alias window opens, with the WWNs tab selected.
4. Enter a name for the zone alias in the Zone Alias Name box.
5. Select the members to add to the zone alias:
   a. Click the **WWNs** tab, select **WWNs**, and click **Add NWwn** to add the node WWN, or click **Add PWwn** to add the port WWN.

      You can also enter a WWN in the Any WWN box and click **Add**.
   b. Click the **Domain, Port** tab, select the domains or ports, and click **Add**.

      You can also enter a domain and port in the Any Domain and Port boxes and click **Add**.

      The Domains in the Fabric area displays all the domains and ports that are available to be added to the zone alias. As each domain or port is added, it disappears from the list of available domains and ports and appears in the Members list.

    c. Click the **iSCSI Names** tab, select names, and click **Add iSCSI Name**.

       You can also enter an iSCSI name in the Any iSCSI Name box and click **Add**.

       Only iSCSI initiators are displayed. Each iSCSI initiator has a WWN assigned to it. These WWNs are not displayed in the WWNs tab, however.

       You must configure a Challenge-Handshake Authentication Protocol (CHAP) secret for the devices in the zone to establish communication. See "Configuring CHAP" on page 100 for more information.

6. Verify that the Zone Alias Members to be added list contains the correct members.

7. Click the **Remove** button to remove members if necessary.

8. Click **OK**.

    The new zone alias is created and is displayed in the Zone Aliases tab.

Cloning a zone alias

Selecting the clone option creates an exact duplicate of an existing zone alias and assigns a new name to the duplicate.

Cloning a zone alias is useful if you want to create a new zone alias that is similar to an existing one. You can create a copy of the existing zone alias and then edit the copy, rather than creating the new zone alias from scratch. Use the following procedure to clone a zone alias:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.

2. Click the **Zone Aliases** tab.

3. Select the zone alias to clone.

4. Click **Clone** in the task bar.

5. Enter a name for the new zone in the New name box of the Clone Zone Alias window.

6. Click **OK**.

    The new zone alias is created and is displayed in the Zone Aliases tab.

Renaming a zone alias

Each zone alias must have a unique name. Use the following procedure to rename a zone alias:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.

2. Click the **Zone Aliases** tab.

3. Select the zone alias to rename.

4. Click **Rename** in the task bar.

5. Enter the new name for the zone alias in the New name box of the Rename Zone Alias window.

6. Click **OK**.

    The renamed zone alias is displayed in the Zone Aliases tab.

Modifying a zone alias

Modifying a zone alias can involve the following tasks:

- Adding zone alias members
- Removing zone alias members
- Renaming the zone alias

The following procedure includes all these tasks:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.

2. Click the **Zone Aliases** tab.

3. Click the name (hyperlink) of the zone alias to modify.

    The zone alias drill-down page opens.

4. To add zone alias members:
   a. Click **Add Zone Alias Members** in the Zone Alias Members task bar.
   b. Click the **WWNs** tab, select **WWNs**, and click **Add NWwn** to add the node WWN, or click **Add PWwn** to add the port WWN.

      You can also type a WWN in the Any WWN box and click **Add**.
   c. Click the **Domain, Port** tab, select the domains or ports, and click **Add**.

      You can also enter a domain and port in the Any Domain and Port boxes and click **Add**.

      The Domains in the Fabric area displays all the domains and ports that are available to be added to the zone alias. As each domain or port is added, it disappears from the list of available domains and ports and appears in the Members list.
   d. Click the **iSCSI Names** tab, select names, and click **Add iSCSI Name**.

      You can also enter an iSCSI name in the Any iSCSI Name box and click **Add**.

      Only iSCSI initiators are displayed. Each iSCSI initiator has a WWN assigned to it. These WWNs are not displayed in the WWNs tab, however.

      You must configure a CHAP secret for the devices in the zone to establish communication. See "Configuring CHAP" on page 100 for more information.
   e. Verify that the Zone Alias Members to be added list contains the correct members.
   f. Click the **Remove** button to remove members, if necessary.
   g. Click **OK**.
5. To remove zone alias members:
   a. Select the zone alias members to delete.
   b. Click **Remove Zone Alias Members** in the Zone Alias Members task bar.
   c. Click **Yes** in the Confirmation window.
6. To rename the zone alias:
   a. Click **Rename** in the task bar.
   b. Enter the new name for the zone alias in the New name box of the Rename Zone Alias window.
   c. Click **OK**.

   The changes to the zone alias are displayed in the zone alias drill-down page.

Deleting a zone alias

Use the following procedure to delete a zone alias. Deleting a zone alias does not affect the effective zone configuration.

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Aliases** tab.
3. Select the zone alias to delete.
4. Click **Delete** in the task bar.
5. Click **Yes** in the confirmation window.

Managing zones

The Zones tab in the Zoning page displays a list of the zones in the fabric and provides tasks for managing those zones (see Figure 22).

From this tab, you can create, rename, delete, clone, and save zones. The procedures for these tasks are described next.

📝 **NOTE:** An asterisk at the end of a zone name indicates that the zone is a member of the effective zone configuration. You cannot rename, modify, or delete these zones.
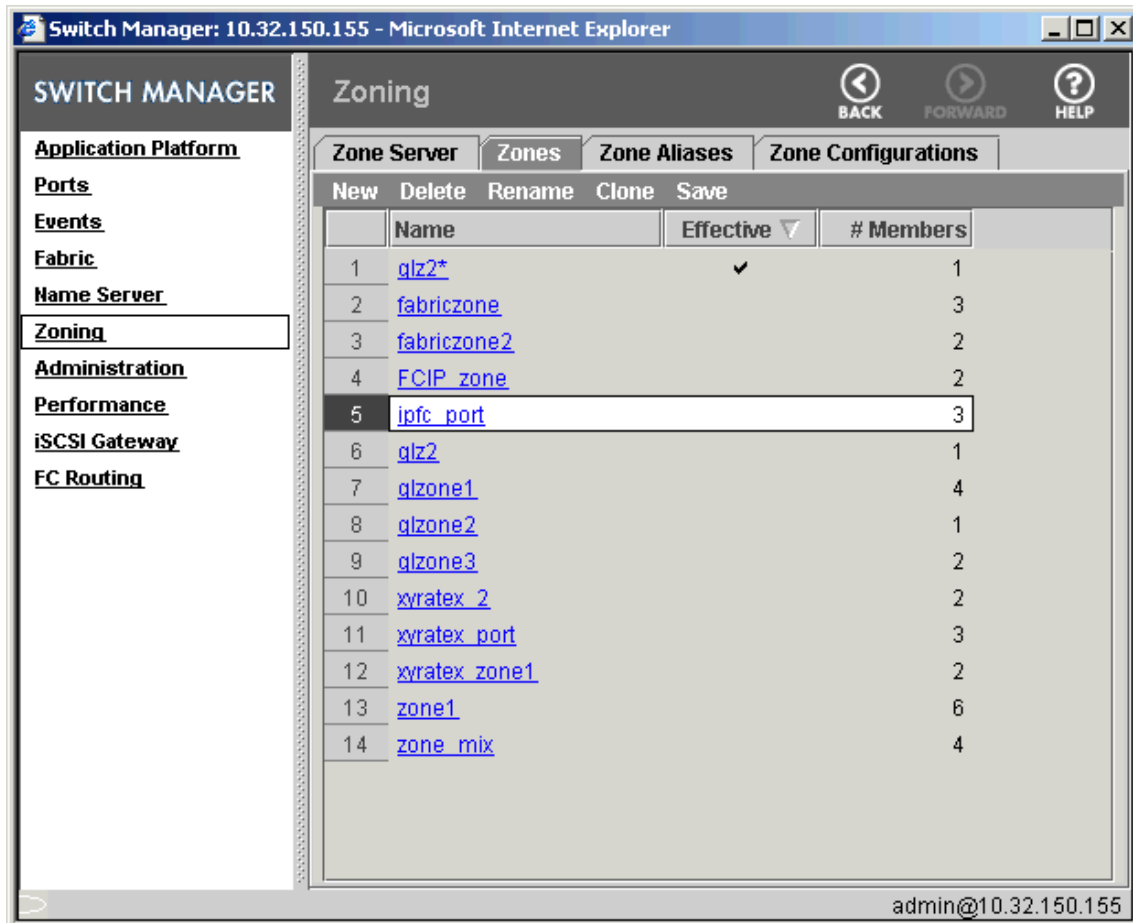
Figure 22 Zoning page with Zones tab selected

Creating a zone

You can specify members of a zone using the following methods:

- Alias names
- WWNs (devices)
- Switch domain and port area number pairs, for example, 2, 20
- iSCSI names

Use the following procedure to create a zone:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zones** tab.
3. Click **New** in the task bar.

    The New Zone dialog box opens with the Aliases tab selected, as shown in Figure 23.
4. Enter a name for the zone in the Zone Name box.
5. Select the members to add to the zone:

    a. Click the **Aliases** tab, select aliases, and click **Add**.

    b. Click the **WWNs** tab, select **WWNs**, and click **Add NWwn** to add the node WWN, or click **Add PWwn** to add the port WWN.

    You can also enter a WWN in the Any WWN box and click **Add**.

c. Click the **Domain, Port** tab, select the domains or ports, and click **Add**.

You can also enter a domain and port in the Any Domain and Port boxes and click **Add**.

The Domains in the Fabric area displays all the domains and ports that are available to be added to the zone. As each domain or port is added, it disappears from the list of available domains and ports and appears in the Members list.

d. Click the **iSCSI Names** tab, select names, and click **Add iSCSI Name**.

You can also enter an iSCSI name in the Any iSCSI Name box and click **Add**.

Only iSCSI initiators are displayed. Each iSCSI initiator has a WWN assigned to it. These WWNs are not displayed in the WWNs tab, however.

You must configure a CHAP secret for the devices in the zone to establish communication. See "Configuring CHAP" on page 100 for more information.

6. Verify that the Zone Members to be Added list contains the correct members.

7. Click the **Remove** button to remove members, if necessary.

8. Click **OK**.

The new zone is created and is displayed in the Zones tab.

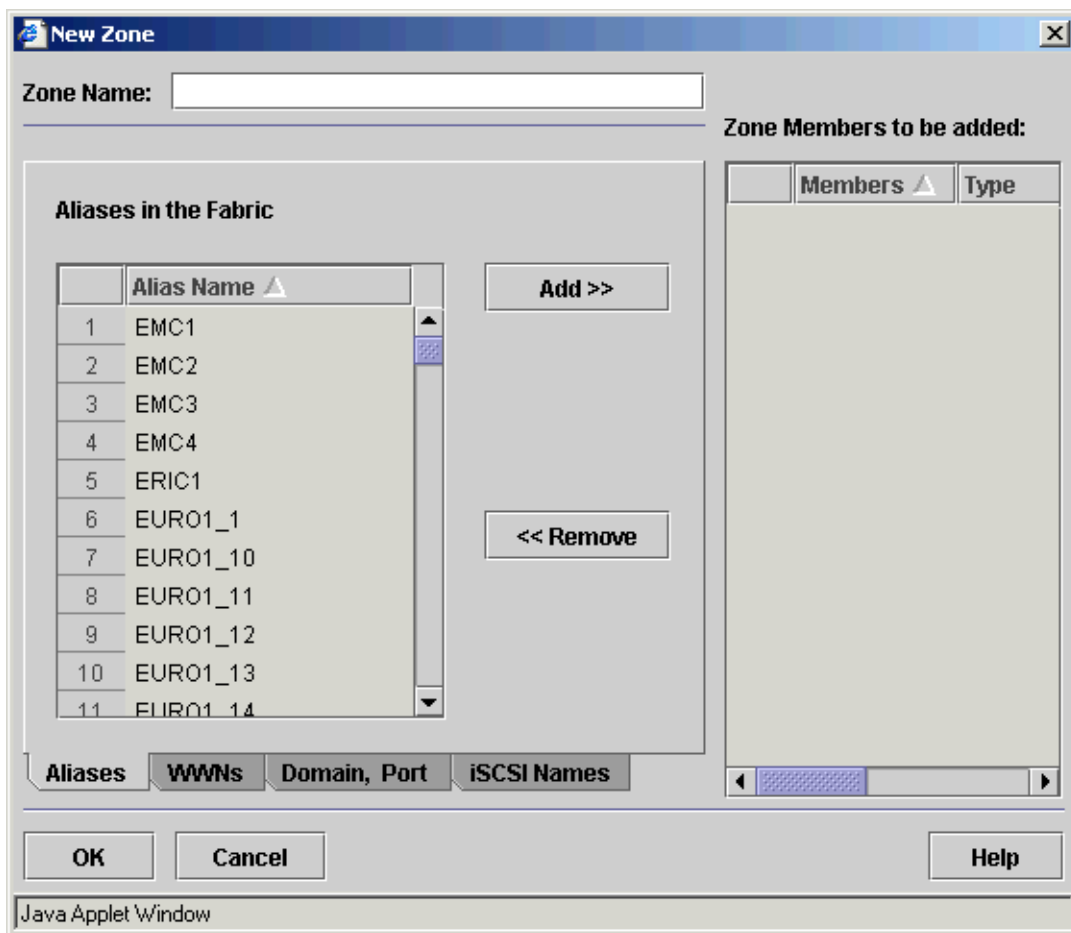**Figure 23** New Zone dialog box

Cloning a zone

Cloning creates an exact duplicate of an existing zone and assigns a new name to the duplicate.

Cloning a zone is useful if you want to create a new zone that is similar to an existing zone. You can create a copy of the existing zone and then edit the copy, rather than creating the new zone from scratch. Use the following procedure to clone a zone:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zones** tab.
3. Select the zone to clone.
4. Click **Clone** in the task bar.
5. Enter a name for the new zone in the New name box of the Clone Zone window.
6. Click **OK**.

   The new zone is created and displayed in the Zones tab.

Renaming a zone

When you rename a zone, a new zone is created and the existing zone is deleted. Because of this, you cannot rename an effective zone (a zone that is part of the effective configuration). Use the following procedure to rename a zone:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zones** tab.
3. Select the zone to rename.
4. Click **Rename** in the task bar.
5. Enter the new name for the zone in the New name box of the Rename Zone window.
6. Click **OK**.

   The renamed zone is displayed in the Zones tab.

Modifying a zone

Modifying a zone can involve the following tasks:

- Adding zone members
- Removing zone members
- Renaming the zone

The following procedure includes all these tasks.

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zones** tab.
3. Click the name (hyperlink) of the zone to modify.

   The zone drill-down page is displayed.
4. To add zone members:
   a. Click **Add Members** in the Zone Members task bar.
   b. Click the **Aliases** tab, select aliases, and click **Add**.
   c. Click the **WWNs** tab, select **WWNs**, and click **Add NWwn** to add the node WWN, or click **Add PWwn** to add the port WWN.

      You can also enter a WWN in the Any WWN box and click **Add**.
   d. Click the **Domain, Port** tab, select the domains or ports, and click **Add**.

      You can also enter a domain and port in the Any Domain and Port boxes and click **Add**.

      The Domains in the Fabric area displays all the domains and ports that are available to be added to the zone. As each domain or port is added, it disappears from the list of available domains and ports and appears in the Members list.

e. Click the **iSCSI Names** tab, select names, and click **Add iSCSI Name**.

You can also enter an iSCSI name in the Any iSCSI Name box and click **Add**.

Only iSCSI initiators are displayed. Each iSCSI initiator has a WWN assigned to it. These WWNs are not displayed in the WWNs tab, however.

You must configure a CHAP secret for the devices in the zone to establish communication. See "Configuring CHAP" on page 100 for more information.

f. Verify that the Zone Members to be added list contains the correct members.

g. Click **Remove** to remove members, if necessary.

h. Click **OK**.

5. To remove zone members:

a. Select the zone members to delete.

b. Click **Remove Members** in the Zone Members task bar.

c. Click **Yes** in the confirmation window.

6. To rename the zone:

d. Click **Rename** in the task bar.

e. Enter the new name for the zone in the New name box of the Rename Zone window.

f. Click **OK**.

The changes to the zone are displayed in the zone drill-down page.

Deleting a zone

You cannot delete zones that are included in the effective zone configuration. Use the following procedure to delete a zone:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.

2. Click the **Zones** tab.

3. Select the zone to delete.

4. Click **Delete** in the task bar.

5. Click **Yes** in the confirmation window.

Managing zone configurations

The Zone Configurations tab in the Zoning page displays a list of the zone configurations in the fabric and provides tasks for managing those zone configurations (see Figure 24).

The effective zone configuration is designated with a check in the Effective column and an asterisk next to the zone configuration name. You cannot alter the effective zone configuration.

A zone configuration with the same name as the effective configuration is also listed. This is a copy of the effective zone configuration. Although you cannot alter the effective zone configuration, you can alter the copy of the effective configuration.

From Zone Configurations tab, you can create, rename, delete, enable, disable, and clone zone configurations. The procedures for these tasks are described next.
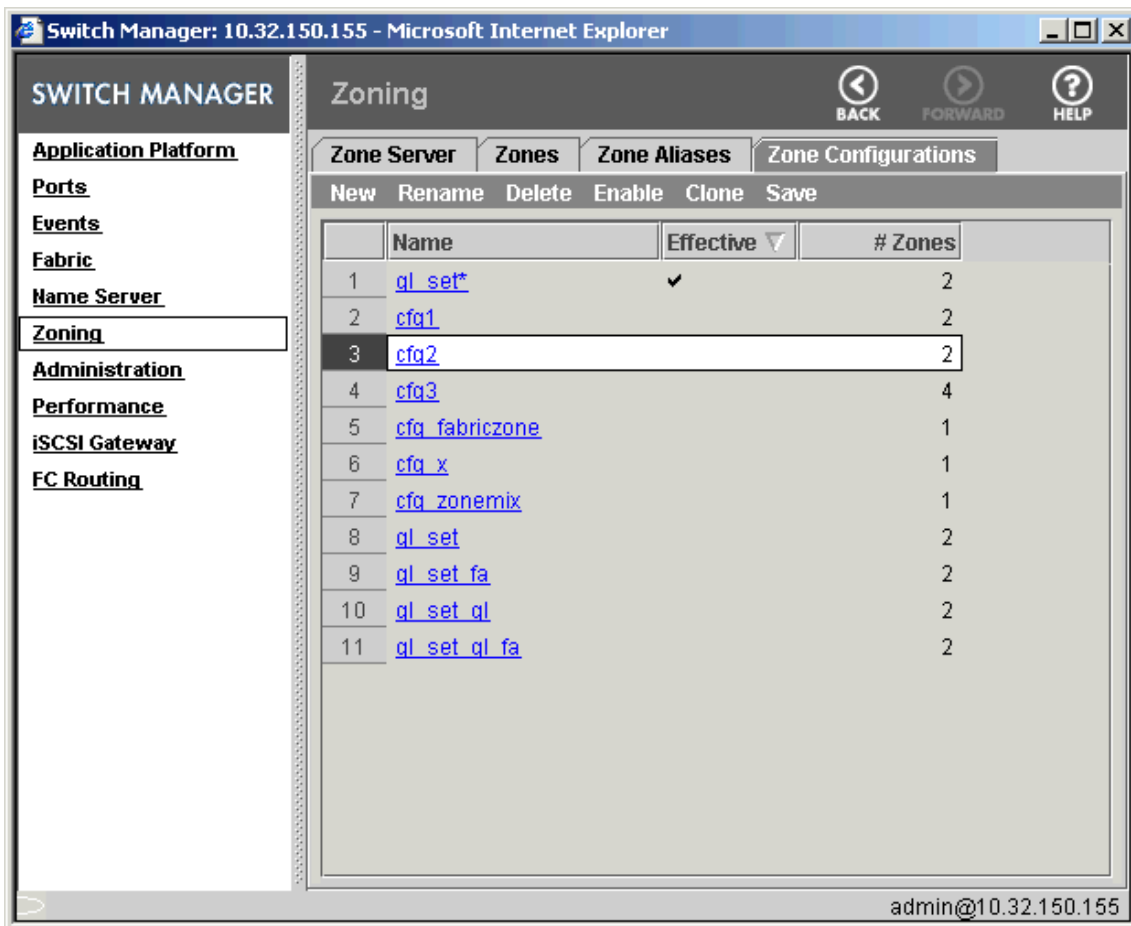
Figure 24 Zoning page with Zone Configurations tab selected

Creating a zone configuration

When you create a zone configuration, that configuration is not activated. You must explicitly enable the zone configuration for it to become the effective configuration. Use the following procedure to create a zone configuration:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Configuration** tab.
3. Click **New** in the task bar.

   The New Zone Configuration window opens.
4. Enter a name for the zone configuration in the Zone Configuration Name box.
5. Select the zones to add to the zone configuration and click **Add**.
6. Verify that the Selected Zones list contains the correct members.
7. Click **Remove** to remove members if necessary.
8. Click **OK**.

   The new zone configuration is created and displayed in the Zone Configurations tab.

Cloning a zone configuration

Cloning creates an exact duplicate of an existing zone configuration and assigns a new name to the duplicate.

Cloning a zone configuration is useful if you want to create a new configuration that is similar to an existing one. You can create a copy of the existing zone configuration and then edit the copy, rather than creating the new configuration from scratch. You cannot clone the effective zone configuration.

Use the following procedure to clone a zone configuration:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Configurations** tab.
3. Select the zone configuration to clone.
4. Click **Clone** in the task bar.
5. Enter a name for the new zone configuration in the New name box of the Clone Zone Configuration window.
6. Click **OK**.

   The new zone configuration is created and is displayed in the Zone Configurations tab.

Renaming a zone configuration

You cannot rename the effective zone configuration. Use the following procedure to rename a zone configuration:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Configurations** tab.
3. Select the zone configuration to rename.
4. Click **Rename** in the task bar.
5. Enter the new name for the zone configuration in the New name box of the Rename Zone Configuration window.
6. Click **OK**.

   The renamed zone configuration is displayed in the Zone Configurations tab.

Modifying a zone configuration

Modifying a zone configuration can involve the following tasks:

- Adding zones
- Removing zones
- Renaming the zone configuration

The following procedure includes all these tasks. You cannot modify the effective zone configuration.

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Configurations** tab.
3. Click the name (hyperlink) of the zone configuration to modify.

   The zone configuration drill-down page is displayed.
4. To add zones to the configuration:
   a. Click **Add Member** in the Members task bar.
   b. Select the zones to add to the zone configuration and click **Add**.
   c. Verify that the Selected Zones list contains the correct members.
   d. Click the **Remove** button to remove members if necessary.
   e. Click **OK**.
5. To remove zones:
   a. Select the zones to remove.
   b. Select **Remove Member** in the Members task bar.
   c. Click **Yes** in the confirmation window.

6. To rename the zone configuration:

    d. Click **Rename** in the task bar.

    e. Enter the new name for the zone configuration in the New name box of the Rename Zone Configuration window.

    f. Click **OK**.

The changes to the zone configuration are displayed in the zone configuration drill-down page.

Deleting a zone configuration

Use the following procedure to delete a zone configuration (you cannot delete the effective configuration):

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Configurations** tab.
3. Select the zone configuration to delete.
4. Click **Delete** in the task bar.
5. Click **Yes** in the confirmation window.

Enabling a zone configuration

Use the enable operation to enable a configuration that has previously been created. Several configurations can reside on a switch at once, and you can quickly alternate between them. For example, you might want to have one configuration enabled during business hours and another enabled overnight. Only one zone configuration can be enabled at a time.

You can enable a zone configuration without having to disable the currently effective one. If a zone configuration is already effective, it is automatically disabled before the new zone configuration is enabled. Use the following procedure to enable a zone configuration:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Configurations** tab.
3. Select the zone configuration to enable.
4. Click **Enable** in the task bar.

   A dialog box opens, asking you to confirm the enable operation. If a zone configuration is already enabled, it is disabled before the selected zone configuration is enabled.
5. Click **Yes** to enable the selected zone configuration or **No** to cancel the request.

Disabling a zone configuration

When you disable the active configuration, the zoning feature is disabled on the fabric and all devices within the fabric can communicate with all other devices. This does not mean that the zoning database is deleted, but only that there is no configuration active on the fabric. Use the following procedure to disable a zone configuration:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Configurations** tab.
3. Select the zone configuration to disable.
4. Click **Disable** in the task bar.

   A dialog box opens, asking you to confirm the disable operation.
5. Click **Yes** to disable the currently enabled zone configuration or **No** to cancel the request.

Configuring zone server attributes

You can configure the following zone server attributes:

- Node WWN checking
- Hard zoning

Use the following procedure to configure zone server attributes:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Server** tab.
3. Click **Edit**.

   The Edit Zone Server Attributes window opens.
4. In the Node WWN Checking section, select one of the following:
   - **Enabled (Consider node WWN members in zones.)**
     When configuring zones, zone aliases, and zone configurations, node WWNs (NWWNs) are available to add as members. For definitions already containing NWWNs as members, these members are included.
   - **Disabled (Ignore node WWN members in zones.)**
     When configuring zones, zone aliases, and zone configurations, NWWNs are not available to add as members. For definitions already containing NWWNs as members, these members are excluded.
5. In the Hard Zoning section, specify whether hard zoning is enabled or disabled.

   See "Zoning enforcement" on page 56 for information about hard zoning.
6. Click **OK**.

Saving zone information

The zone configuration is stored in the configuration file on a switch. This enables you to upload and download the zoning configuration as a text file and export a zone configuration to another switch easily. Use the following procedure to save zone information to persistent storage:

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click **Save** in the task bar of any zoning tab.
3. Click **Yes** in the confirmation window.

   All zones, zone aliases, and zone configurations are saved in persistent storage.

Deleting all zone information

△ **CAUTION:** This procedure removes all zone, zone alias, and zone configuration information from the fabric. This fabric change is persistent.

1. From the Switch Explorer, click the **Zone Administration** icon in the fabric toolbar, or from the Switch Manager, click **Zoning** in the navigation bar.
2. Click the **Zone Server** tab.
3. Click **Purge** in the task bar.
4. Click **Yes** in the confirmation window or **No** to cancel the operation.

   The active zone configuration is automatically disabled before deletion.

6 Using the event log

This chapter provides information on viewing the event log and contains the following sections:

- Event messaging in XPath OS, next
- Viewing the event log, page 72
- Adding and deleting syslog hosts, page 73

Event messaging in XPath OS

Event messages provide information regarding the status of the switch and ports; each message has a severity level. The *event log* saves all messages generated by the system since the last reboot. The *persistent event log* saves messages in nonvolatile memory so that they are saved across reboots and power cycles.

Saving messages to the event log and saving messages to the persistent event log are examples of event actions; another possible event action is reporting messages to the SNMP process. You can modify the actions XPath OS takes when it receives an event message.

Event log

XPath OS maintains an internal event log of all diagnostic and system error messages. Each switch has its own event log. By default, some critical events along with diagnostic events are saved to nonvolatile memory, and all other messages are volatile. Messages not saved to nonvolatile memory are lost over power cycles and reboots.

The event log is implemented as a circular buffer. When the internal buffers are full, new messages overwrite old messages. For information on event log buffer limits, see the *HP StorageWorks XPath OS 7.4.x system error messages reference guide*.

The Events page of Switch Manager displays event log messages. By default, the page displays all event messages, both volatile event messages (saved in memory) and persistent event messages (saved in nonvolatile memory). For details, see "Viewing the event log" on page 72.

Event log message levels

There are six severity levels for event messages, ranging from Panic to Debug. Use the definitions in Table 3 as general guidelines for troubleshooting. Review each event description thoroughly before taking action.

Table 3 Event message levels

Event level	Description
0 = Panic	Panic messages indicate that a specific software subsystem has detected a fatal or unrecoverable error condition. Examples are memory allocation failure, system call failure, and software detection of problems with the ASIC or with hardware subsystems. These errors usually indicate partial or complete failure of a subsystem.
1 = Critical	Critical messages indicate that the software has detected serious problems that eventually cause a partial or complete failure of a subsystem if not corrected immediately. A power supply failure, for example, or a rise in temperature must receive immediate attention. Some of the critical errors might overlap in severity with the panic messages.
2 = Error	Error messages indicate error conditions that do not significantly affect overall system functionality. For example, error messages might indicate time-outs on certain operations, failures of certain operations after retries, invalid parameters, or failures to perform requested operations.
3 = Warning	Warning messages highlight current operating conditions that should be checked before they cause failures. For example, a power supply failure in a redundant system relays a warning that the system is no longer operating in redundant mode, and that the failed power supply should be replaced or fixed.

Table 3 Event message levels (continued)

Event level	Description
4 = Info	Info messages report the current status of the system components other than error status. For example, detecting on and off line status of a fabric port.
5 = Debug	Debug messages are for debugging use only. They are produced by code inserted by the vendor to inform the user that a suspected problem has occurred.

Viewing the event log

You can view all the events in the event log or you can limit the events that are displayed, based on certain criteria, such as type, severity level, or time of occurrence. (The time of occurrence is based on the host system time, not the switch time.) Use the following procedure to view the event log:

1. Access the Switch Manager.
2. Click **Events** in the navigation bar.

   The Events page displays all the event messages in the event log, as shown in Figure 25.
3. Optional: Choose a value from the Select time to be shown for events drop-down list.

   You can choose to display the switch time of the events, the local time of the events, or both.

Figure 25 Events page

Filtering the displayed events

An event must meet all selected criteria to be displayed in the table.

1. Access the Switch Manager.
2. Click **Events** in the navigation bar.

3. Click **Filter** in the task bar.
4. Select the filter criteria:
   - To show all events occurring after a specified date and time:
     a. Select the **From** checkbox to activate this filter.
     b. Select the starting date from the drop-down menu in the leftmost From box.

        The drop-down menu contains a calendar from which you can select the date. You can also enter the date in the boxes.
     c. Enter the starting time in the rightmost From box.

        The time is in the format *hh:mm.ss*, where *hh* is an integer between 1 and 12 and *mm* and *ss* are integers between 0 and 59.
     d. Select **AM** or **PM**.
   - To show only events occurring before a specified date and time:
     a. Select the **To** checkbox to activate this filter.
     b. Select the ending date from the drop-down menu in the leftmost From box.

        The drop-down menu contains a calendar from which you can select the date. You can also enter the date in the box.
     c. Enter the ending time in the rightmost From box. The time is in the format *hh:mm.ss*, where *hh* is an integer between 1 and 12 and *mm* and *ss* are integers between 0 and 59.
     d. Select **AM** or **PM**.
   - To specify a severity level filter, select a level from the Level drop-down menu. Severity levels are listed in ascending severity order, with Debug as the lowest level and Panic the highest.
   - To show only events of a specified type, select a type from the Type drop-down menu. Select **Active Events** or **Persistent Events**.
5. Click **OK** to create the new events filter.

Adding and deleting syslog hosts

The syslog host is the server that is running the syslog daemon. Events on the MP Router are sent to the syslog daemon on the specified host.

The syslog daemon reads and forwards system messages to the appropriate log files and users, depending on the system configuration. When one or more IP addresses are configured, the MP Router forwards system error log entries to the syslog on the specified servers.

Use the following procedure to add a syslog host:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Network Config** tab (see).
4. Click **Add** in the Syslog Hosts task bar.
5. Enter a valid IP address for the syslog host.
6. Click **OK**.

Use the following procedure to delete a syslog host:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Network Config** tab (see).
4. Select the syslog host to delete in the Syslog Hosts table.

   The syslog hosts are identified by IP addresses.
5. Click **Delete** in the Syslog Hosts task bar.
6. Click **Yes** in the confirmation window.

7 Managing Fibre Channel frame routing

There are two major aspects of Fibre Channel frame routing that you can control: whether frames must be delivered in order and whether dynamic load-sharing path calculations are permitted. You can also view path and port routing information.

This chapter provides information about frame routing and contains the following sections:

- Managing routing with Advanced Web Tools, next
- Enabling and disabling in-order frame delivery, page 76
- Enabling and disabling dynamic load sharing, page 76
- Viewing FSPF routes, page 77
- Managing static routes, page 78
- Configuring link cost, page 80

Managing routing with Advanced Web Tools

You can monitor and manage routing through the Switch Manager. Click **Administration** in the navigation bar, and then click the **Routing** tab. Figure 26 shows the Administration page with the Routing tab and IOD/DLS subtab selected.
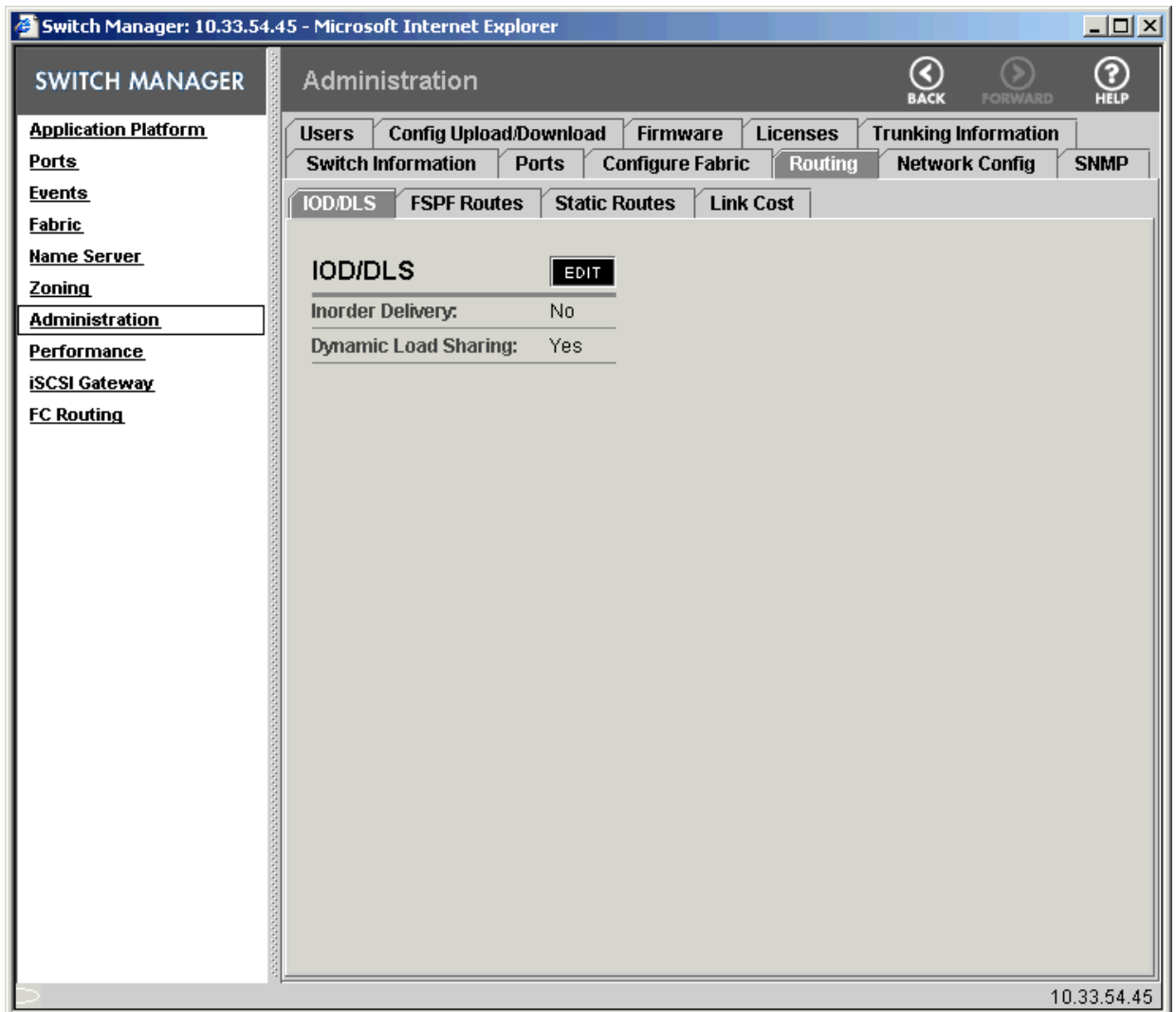

Figure 26 Administration page with Routing tab and IOD/DLS subtab selected

Enabling and disabling in-order frame delivery

In a stable fabric, frames are always delivered in order, even when the traffic between switches is shared among multiple paths. However, when topology changes occur in the fabric (for instance, a link goes down), traffic is rerouted around the failure. When topology changes occur, some frames can be delivered out of order.

Enabling in-order delivery (IOD) guarantees that frames are either delivered in order or dropped. In this case, frames are not delivered out-of-order, even during fabric topology changes. This option should be used with care, because it causes a delay in the establishment of a new path when a topology change occurs. This option should be used only if there are devices connected to the fabric that do not tolerate occasional out-of-order delivery of frames.

The default behavior is for the in-order delivery option to be off. This allows out-of-order delivery of frames during fabric topology changes and enables fast rerouting after a fabric topology change. Use the following procedure to enable or disable in-order frame delivery:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Routing** tab.
4. Click the **IOD/DLS** subtab (see Figure 26 on page 75).
5. Click **Edit**.
6. Select the in-order delivery option:
   - Select **In Order Delivery** to enforce in-order frame delivery during fabric topology changes.
   - Clear **In Order Delivery** to disable the in-order frame delivery.
7. Click **OK**.

Enabling and disabling dynamic load sharing

Dynamic load sharing (DLS) refers to a dynamic distribution of traffic over available paths. Enabling DLS allows load sharing when a fabric change occurs.

Routing is generally based on the incoming port and the destination domain. This means that all the traffic coming in from an E_Port or an Fx_Port (an Fx_Port is either an F_Port or an FL_Port) that is directed to the same remote domain is routed through the same output E_Port.

To optimize fabric routing, when there are multiple equivalent paths to a remote switch, traffic is shared among all the paths. Load sharing is usually recomputed when a switch reboots. If DLS is enabled, load sharing is also recomputed every time a change in the fabric occurs, such as when an E_Port or Fx_Port goes up or down.

If DLS is turned off, load sharing is performed only at boot time, when an Nx_Port comes up, or when a new ISL comes up. Optimal load sharing is rarely achieved with this setting.

DLS is enabled by default. DLS and link cost are not directly related. Routes are calculated based on the link cost. If there are multiple routes to a destination domain and if DLS is enabled, each local device or E-Port gets one of the routes.

📝 **NOTE:**   Trunking overrides the DLS setting.

Use the following procedure to enable or disable DLS:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Routing** tab.
4. Click the **IOD/DLS** subtab (see Figure 26 on page 75).
5. Click **Edit**.

6. Select the load sharing option:
   - Select **Dynamic Load Sharing** to enable DLS.
   - Clear **Dynamic Load Sharing** to disable DLS.
7. Click **OK**.

Viewing FSPF routes

The FSPF Routes pane displays the FSPF routes (see Figure 27) and the following information about each route:

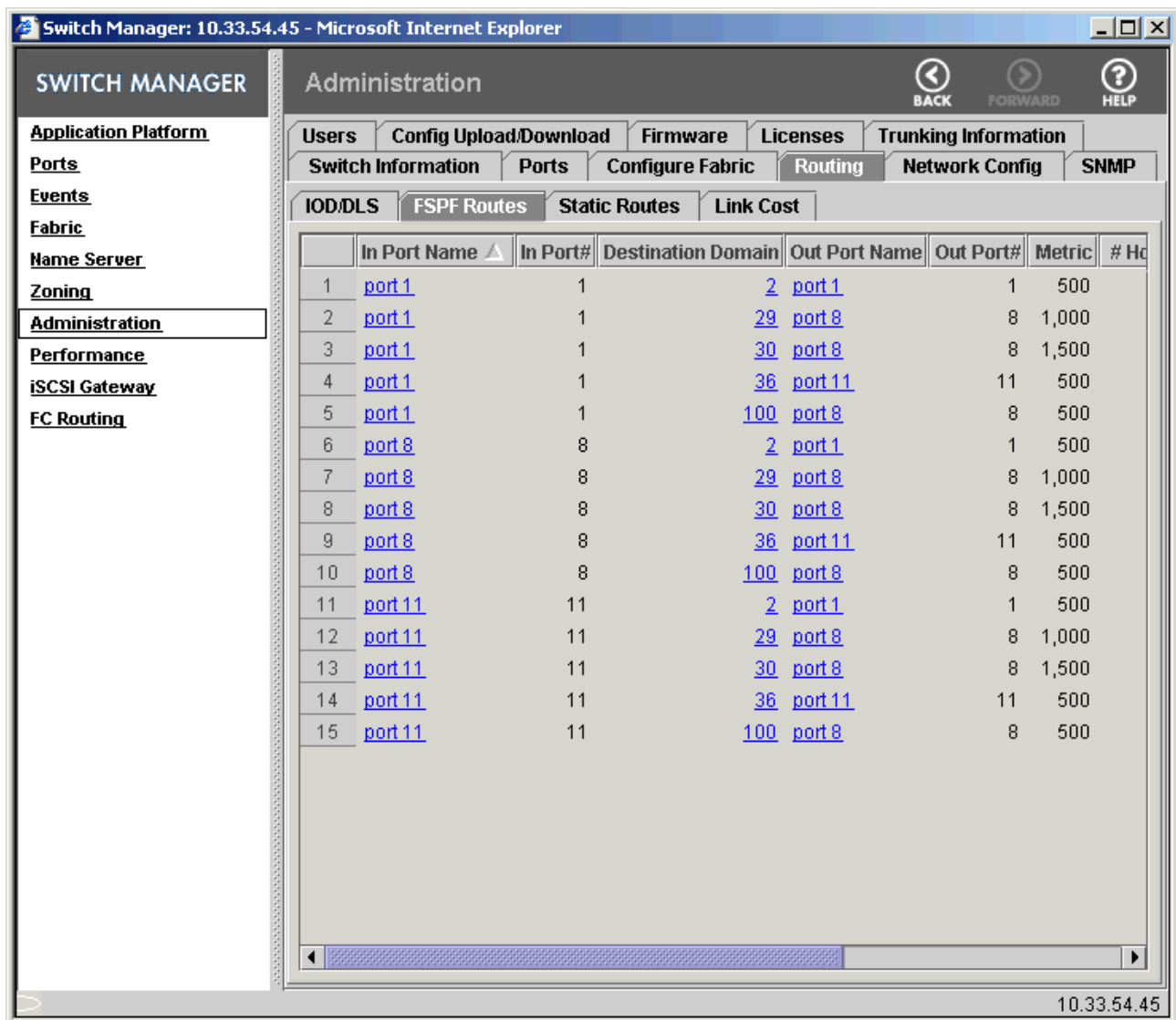|	
In Port Name	The name of the port from which a frame comes.
In Port#	The number of the port from which a frame comes.
Destination Domain	The destination domain of the incoming frame.
Out Port Name	The name of the port to which an incoming frame is forwarded to reach the destination domain.
Out Port#	The number of the port to which the incoming frame is forwarded to reach the destination domain.
Metric	The cost of reaching the destination domain (the sum of the costs of all the ISLs traversed by the path).
# Hops	The maximum number of hops to reach the destination domain.
Flags	Specifies whether this route is dynamic or static. A dynamic route is discovered automatically by the FSPF path-selection protocol. A static route is assigned from the Static Routes tab.
Next Domain	The domain of the next hop, which is the domain ID of the switch to which the Out Port is connected.
Next Port	The port number of the next hop, which is the port number on the switch to which the Out Port is connected.

Figure 27 Administration page with Routing tab and FSPF Routes subtab selected

Managing static routes

You can view and manage static routes through the Static Routes subtab, as shown in Figure 28. The Static Routes pane displays the following information about each route:

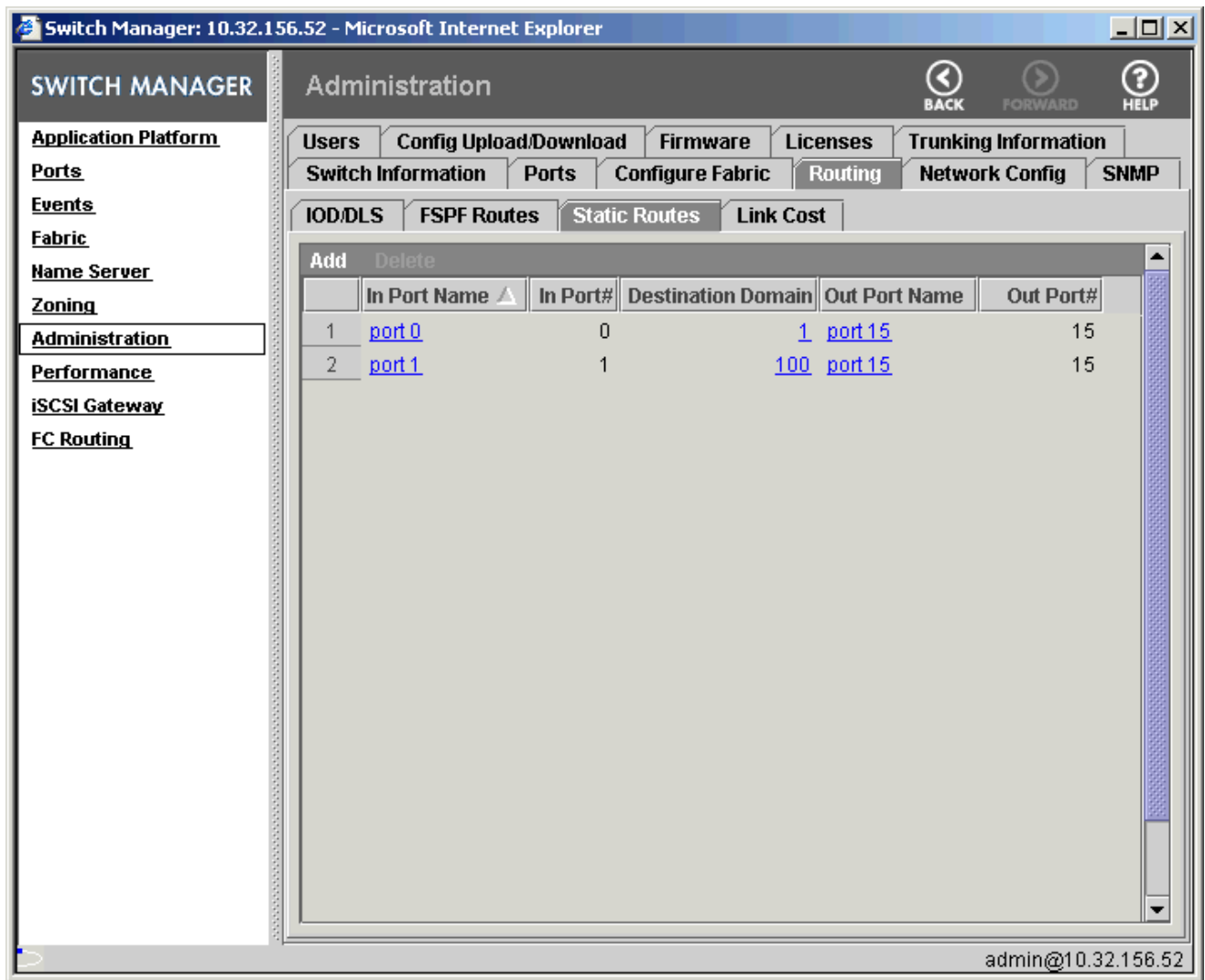|	
In Port Name	The name of the port from which a frame comes.
In Port#	The number of the port from which a frame comes.
Destination Domain	The destination domain of the incoming frame.
Out Port Name	The name of the port to which an incoming frame is forwarded to reach the destination domain.
Out Port#	The number of the port to which the incoming frame is forwarded to reach the destination domain.

Figure 28 Administration page with Routing tab and Static Routes subtab selected

Configuring a static route

Use the following procedure to add a static route:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Routing** tab.
4. Click the **Static Routes** subtab.
5. Click **Add** in the task bar.
   The Add Static FC Route dialog box opens.
6. Select the input port from the drop-down list.
7. Enter the destination domain ID.
8. Select the output port from the drop-down list.
9. Click **OK**.

Deleting a static route

Use the following procedure to delete a static route:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Routing** tab.

4. Click the **Static Routes** subtab.
5. Select the route to delete.
6. Click **Delete** in the task bar.
7. Click **Yes** in the confirmation window.

Configuring link cost

The cost of a link is used to determine the least-costly path for a frame from the source to the destination switch. The cost of a path is the sum of the costs of all the ISLs traversed by that path.

Every ISL has a default cost that is inversely proportional to its bandwidth. For a 1-Gbit/sec ISL, the default link cost is 1,000; for a 2-Gbit/sec ISL, the default link cost is 500.

Although you can also configure link cost when you configure a port, the following procedure is useful for configuring the link cost of multiple ports at the same time:

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Routing** tab.
4. Click the **Link Cost** subtab (see Figure 29).
5. Select the appropriate port.
   You can select more than one port by pressing Shift-click and Ctrl-click.
6. Click **Edit** in the task bar.
   The Edit Link Cost dialog box opens.
7. Select the link cost:
   • Click **Auto** to automatically set the link cost to the default link cost, which is based on port speed (for a 1-Gbit/sec ISL, the link cost is 1000; for a 2-Gbit/sec ISL, the link cost is 500).
   • Click **Custom** and enter the static link cost. You can enter an integer from 1 to 65,535.
8. Click **OK**.

Figure 29 Administration page with Routing tab and Link Cost subtab selected

8 Monitoring performance

This chapter contains the following sections:

- Monitoring performance with Advanced Web Tools, next
- Configuring the performance table, page 84
- Refreshing the ports and counters table, page 85
- Changing the autorefresh interval, page 85
- Changing the counter values, page 85
- Configuring performance charts, page 86

Monitoring performance with Advanced Web Tools

You can monitor performance through the Switch Manager. Click **Performance** in the navigation bar to access the Performance page. The Performance page displays performance statistics for selected ports. You can customize the ports and the counters that are to be displayed. You can also view performance statistics in tabular format or in charts.

Figure 30 shows the Performance page with the Counters tab selected. Figure 31 shows the Performance page with the Charts tab selected.
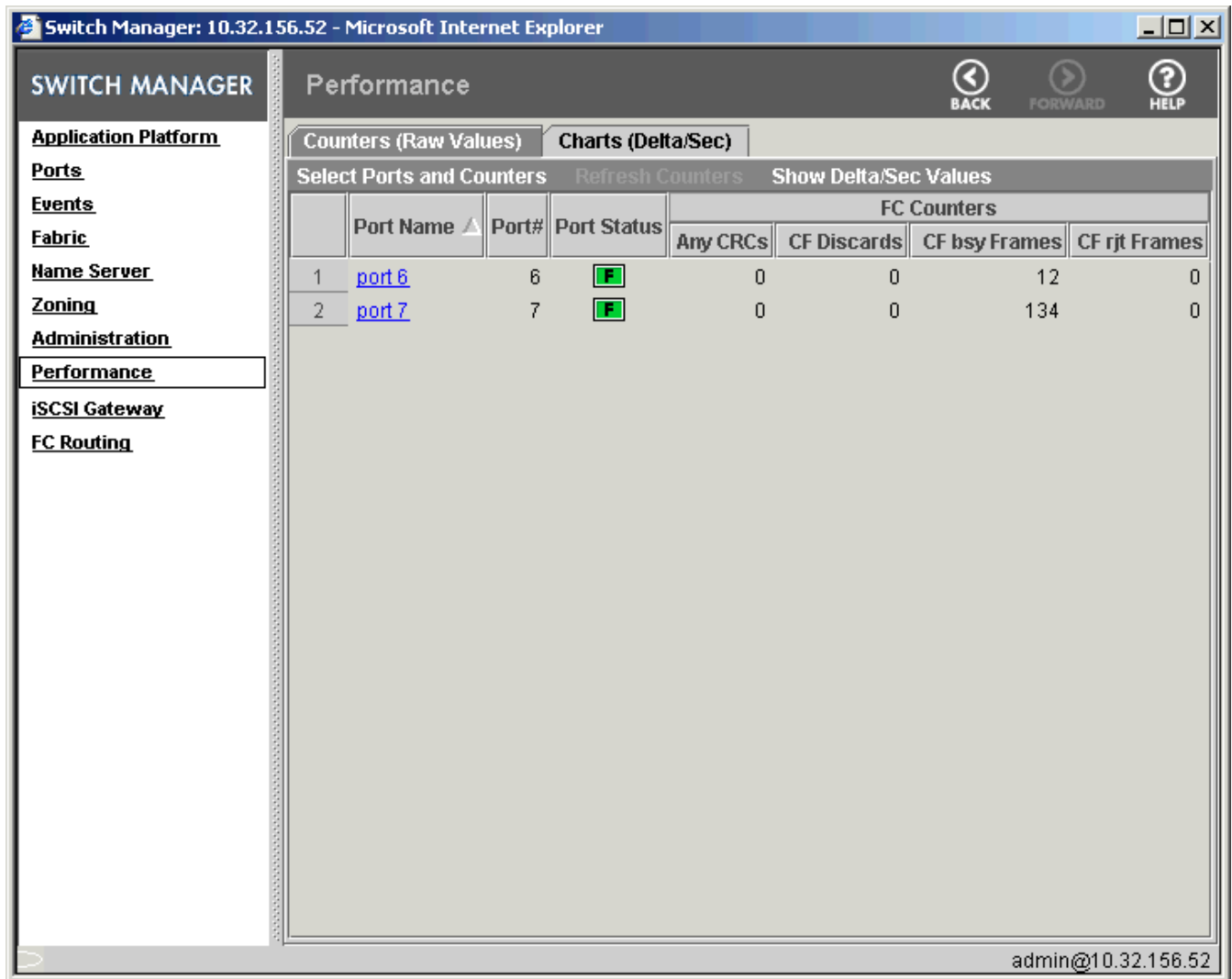

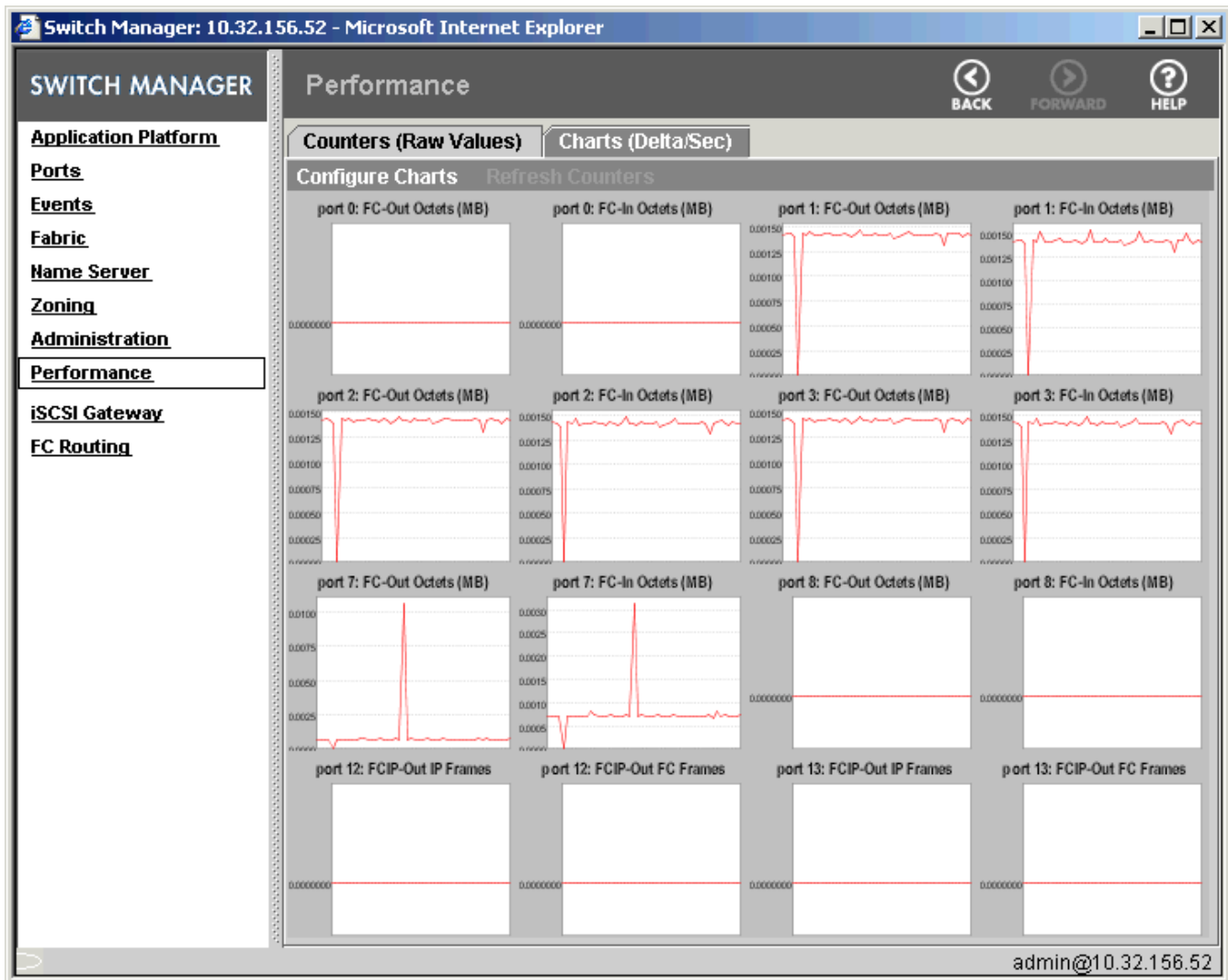**Figure 30** Performance page with Counters tab selected

Figure 31 Performance page with Charts tab selected

Configuring the performance table

You can customize the performance information to be displayed by selecting the ports you want to monitor and the counters to be included in the table.

Selecting the ports and counters to monitor

1. From the Switch Explorer, click the **Perf** icon in the Switch View, or from the Switch Manager, click **Performance** in the navigation bar.
2. Click the **Counters** tab.
3. Click **Select Ports and Counters** in the task bar.
4. Select the ports for which you want to gather performance statistics.
5. Click **Next**.
6. Select the counters you want to include in the ports and counters displays.
7. Click **Next**.
8. Select the **Enable Auto-Refresh** checkbox to automatically refresh the displays. Clear this checkbox to disable autorefresh.
9. Enter the refresh interval in seconds, if autorefresh is enabled.
10. Click **Finish**.

   The selected ports and counters are displayed in the Performance page.

Refreshing the ports and counters table

If the Refresh Counters task is grayed out, it means that autorefresh is enabled and the display is refreshed after a specified number of seconds. To disable autorefresh or to change the refresh interval, see the section "Changing the autorefresh interval," next.

Refreshing the counter display and charts

1. From the Switch Explorer, click the **Perf** icon in the Switch View or from the Switch Manager, click **Performance** in the navigation bar.
2. Click the **Counters** tab or the **Charts** tab.
3. Click **Refresh Counters** in the task bar.

    The counters in the table and charts are updated.

Changing the autorefresh interval

The autorefresh settings are applied to counters and charts displayed anywhere in the Advanced Web Tools application.

Use the following procedure to change the refresh interval from the Counters tab. You can also change the interval using the Configure Charts task in the Charts tab.

1. From the Switch Explorer, click the **Perf** icon in the Switch View or from the Switch Manager, click **Performance** in the navigation bar.
2. Click the **Counters** tab.
3. Click **Select Ports and Counters** in the task bar.
4. Click **Next** in the dialog box.
5. Click **Next** again.
6. Select the **Enable Auto-Refresh** checkbox to automatically refresh the displays. Clear this checkbox to disable autorefresh.
7. Enter the refresh interval in seconds, if autorefresh is enabled.
8. Click **Finish**.

Changing the counter values

The counter values displayed in the Performance page can be either raw counter values or Delta/Sec values. A raw counter value is the total count for a counter since the MP Router was booted.

Delta/Sec values are calculated as follows:

$$(y2 - y1) / (t2 - t1)$$

where $y1$ and $y2$ are successive raw counter values, and $t1$ and $t2$ are the associated time stamps at which the $y1$ and $y2$ values were obtained from the MP Router.

By default, Delta/Sec values are shown in the Counters tab opens.

Use the following procedure to change the counter values that are displayed:

1. From the Switch Explorer, click the **Perf** icon in the Switch View, or from the Switch Manager, click **Performance** in the navigation bar.
2. Click the **Counters** tab.
3. Click **Show Raw Counters** or **Show Delta/Sec Counters** in the task bar to toggle between the two displays.

    The type of counter that is displayed is shown in the Counters tab.

Configuring performance charts

The number of charts displayed depends on the chart configuration you select. You can select multiple charts to be displayed or a single chart to display all the performance statistics.

The maximum number of charts that can be displayed is 16. If you select a combination of ports and counters that results in a number of charts exceeding the maximum, an error message appears, asking you to reduce the number of ports and counters selected. For example, if you select 10 ports and 2 counters and then select **the One chart per port and counter option,** the resulting number of charts would be 20, which exceeds the maximum. In this case, deselect some of the items (for example, deselect one counter) to generate the allowable number of charts. Alternatively, select a different type of layout that results in fewer charts being generated.

The maximum number of data sets that can be displayed is 32. A *data set* is defined as a line on a chart. The number of data sets is determined by the following formula:

    number_of_data_sets = number_of_counters * number_of_charts

For example, you can have 1 chart with 32 counters, or 8 charts with 4 counters each, or 6 charts with 5 counters each.

📝 **NOTE:**   The charts can display up to 16 different colors. If the number of data sets is greater than 16, the colors are reused, and it might become difficult to distinguish between data sets.

Keep the chart and data set maximums in mind when selecting ports, counters, and chart layout in the following procedure.

1. From the Switch Explorer, click the **Perf** icon in the Switch View or from the Switch Manager, click **Performance** in the navigation bar.
2. Click the **Charts** tab.
3. Click **Configure Charts** in the task bar.

    The Configure Charts window opens.
4. Select the ports you want to appear in the chart displays.
5. Click **Next**.
6. Select the types of counters to appear in the chart displays.
7. Click **Next**.
8. Select the type of layout to use for the charts:
    - **One chart per port** displays a separate chart for each selected port. All selected counters are included on each port chart.
    - **One chart per counter** displays a separate chart for each counter type. All ports are included in each chart.
    - **One chart per port and counter** displays a separate chart for each counter type for each selected port. Each chart includes one port and one counter for that port.
    - **One chart for all ports and counters** displays a single chart that includes all selected ports and counters.
9. Click the **Enable Auto-Refresh** box to automatically refresh the displays.
10. If you chose to turn on autorefresh, type the refresh interval in seconds.
11. Click **Finish**.

    The charts appear in the Charts tab. You can right-click a graph to zoom in and out, change the properties of the graph, or print the graph.

9 Using the FC-FC Routing service

This chapter provides the procedures for managing Fibre Channel routing using Advanced Web Tools. It contains the following sections:

- Managing FC-FC Routing with Advanced Web Tools, next
- Setting up a meta-SAN with an MP Router, page 92
- Configuring a backbone fabric, page 92

For background information on Fibre Channel routing, see the *HP StorageWorks XPath OS 7.4.x administrator guide*.

Managing FC-FC Routing with Advanced Web Tools

You can monitor and manage FC-FC Routing and EX_Ports through the Switch Manager. Click **FC Routing** in the navigation bar to access the FC Routing page. Figure 32 shows the FC Routing page with the General tab selected. The General tab displays basic information about FC-FC Routing.
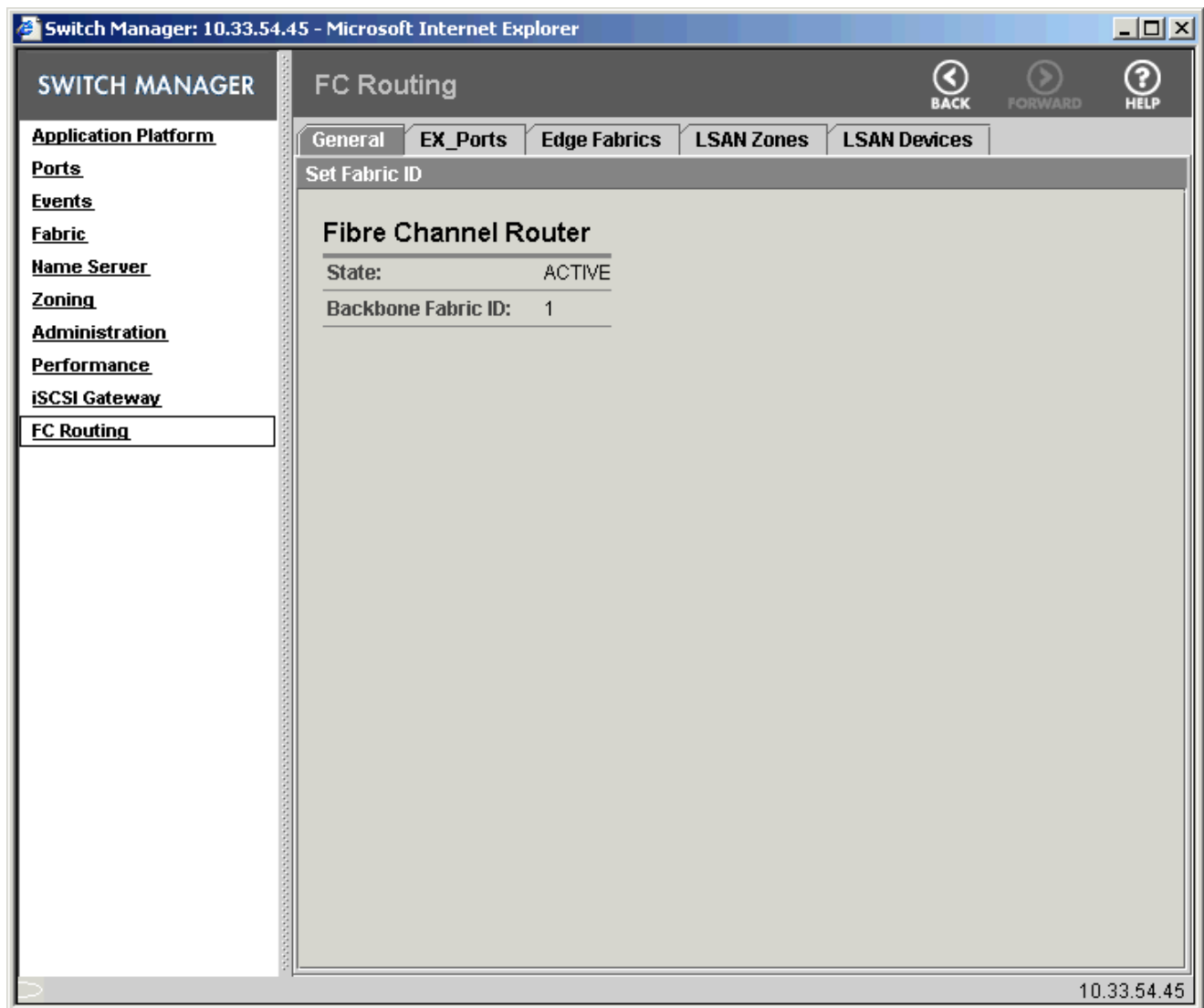
Figure 32 FC Routing page with the General tab selected

Viewing and configuring EX_Port information

The EX_Ports tab (see Figure 33) displays the EX_Ports, including configuration and status information. You can also view this information from the Ports page.

To configure the EX_Ports, use the same procedures described in "Managing ports" on page 45, The EX_Port tasks that are listed in the task bar are the same as those tasks described in "Managing ports" on page 45.

For more detailed information on a specific port, click the port name to display a drill-down page for that port, as shown in Figure 4 on page 18. The name of the port is listed at the top of the page and is also indicated in the port diagram. The port drill-down page has several tabs that display additional information about the port.

You can perform port management tasks for a single port from the port drill-down page. You can perform these same tasks on multiple ports from the Ports or FC Routing pages. These pages allow you to select multiple ports, for example, if you want to configure multiple ports at the same time.

Figure 33 FC Routing page with EX_Ports tab selected

Viewing edge fabric information

The Edge Fabric tab (see Figure 34) lists all the edge fabrics visible to the MP Router. The table displays the following information about each edge fabric:

ID   The fabric ID of the edge fabric.

Type   The type of edge fabric. Values are Local and Remote.

Edge Domain   The domain name of the edge fabric.

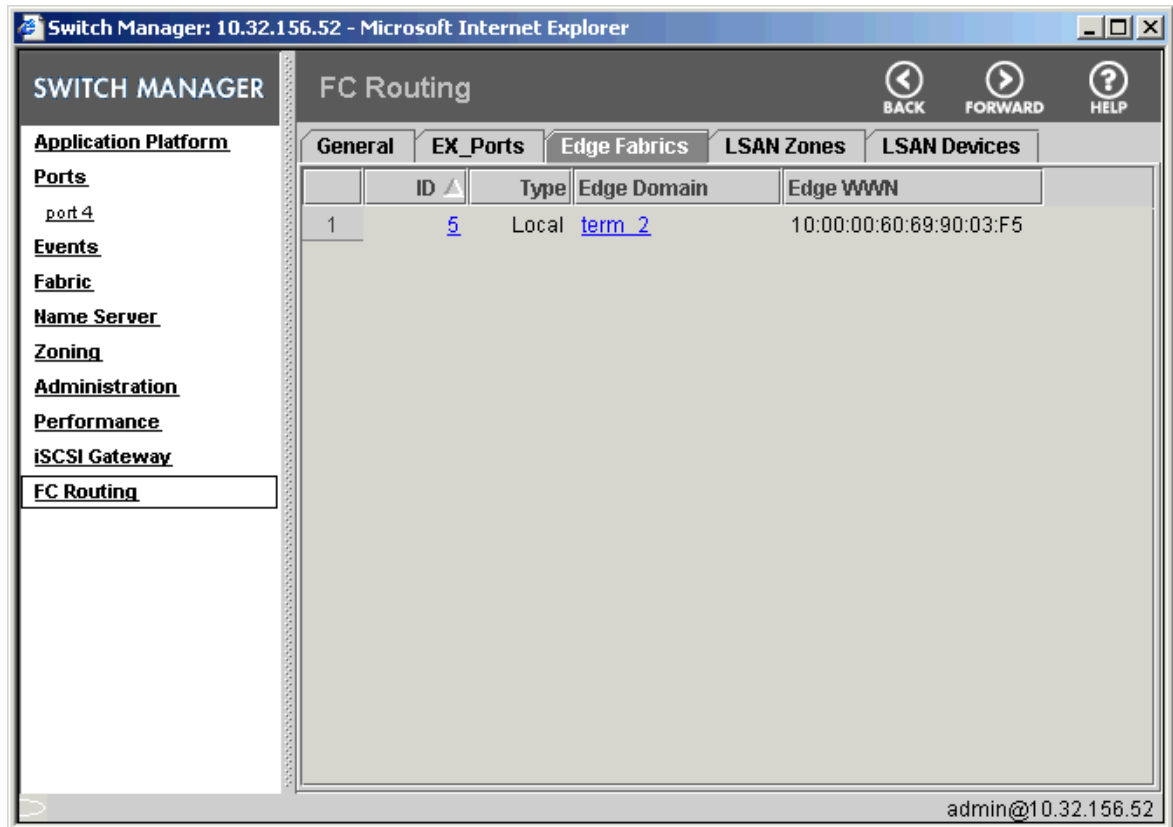Edge WWN   The WWN of the switch of the edge fabric.

Figure 34 FC Routing page with the Edge Fabrics tab selected

Viewing LSAN zones

The LSAN Zones tab (see Figure 35) lists all the LSAN zones. This tab displays the name of each LSAN zone and the ID of the fabric in which it was created.
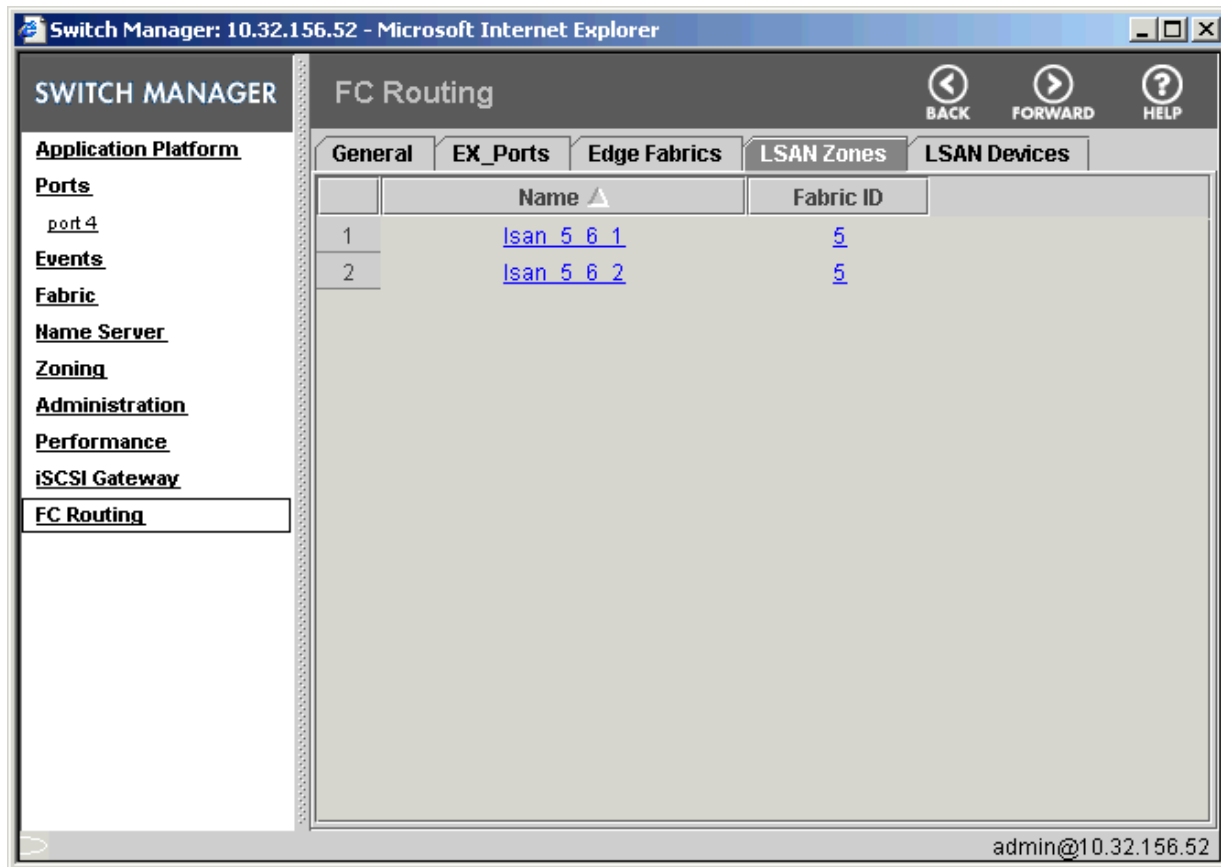
Figure 35 FC Routing page with the LSAN Zones tab selected

Viewing LSAN devices

The LSAN Devices tab (see Figure 36) lists all the LSAN devices. An LSAN device can be a *physical device*, meaning that it physically exists in the fabric, or it can be a *proxy device*. A proxy device represents a real device on another edge fabric. It has a Name Server entry and is assigned a valid port ID. When a proxy device is created in a fabric, the real device is considered to be imported into that fabric. The presence of a proxy device is required for interfabric device communication.

Physical devices

The Physical pane displays the following information about each physical LSAN device:

Port WWN   The WWN of the device port.

Physical Fabric   The fabric ID of the edge fabric to which this LSAN device belongs.

Physical PID   The port ID (PID) of the physical device.

Node WWN   The WWN of the device node.

Vendor   The name of the device vendor.
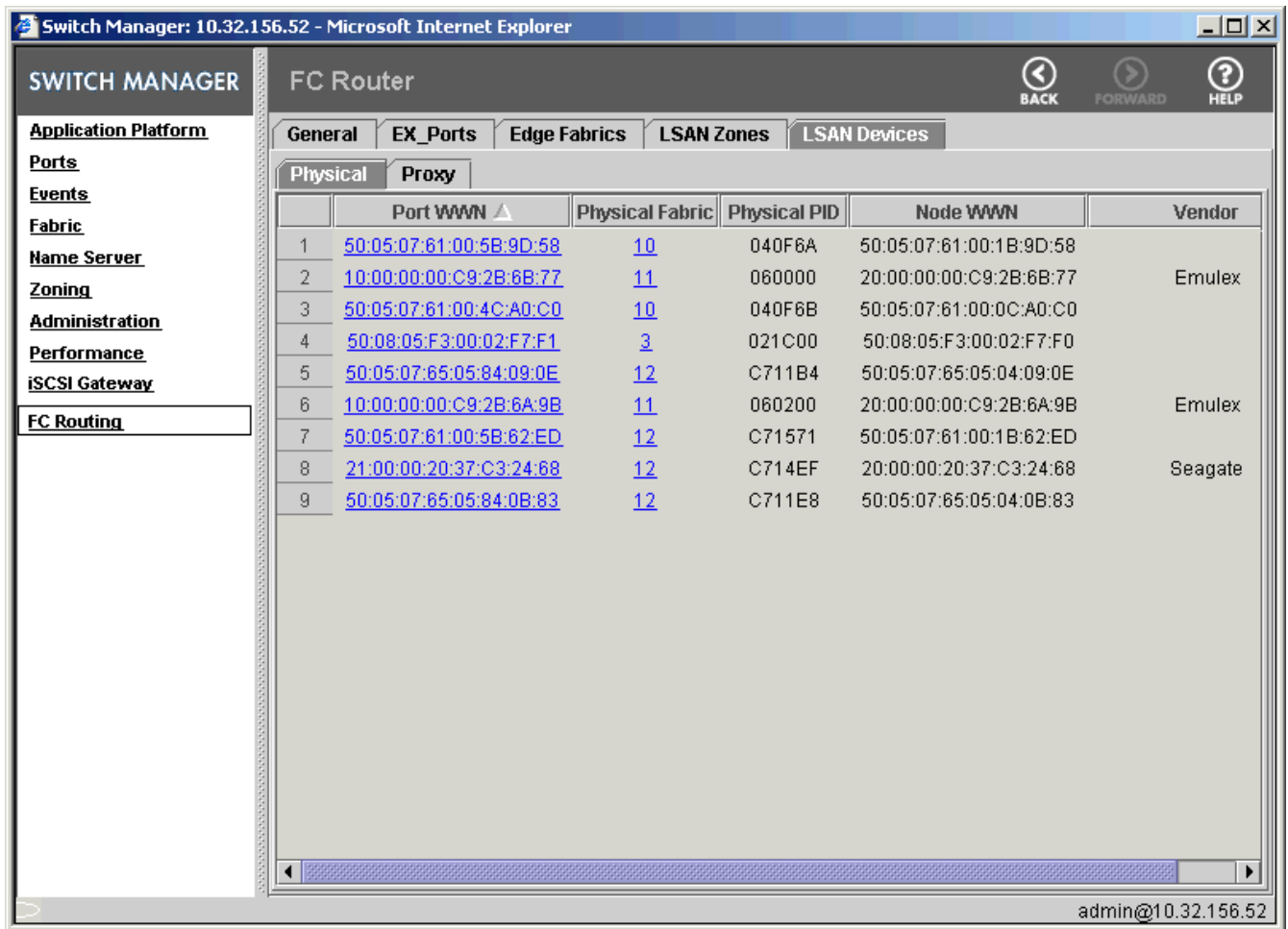
Figure 36 FC Routing page with LSAN Devices tab and Physical subtab selected

Proxy devices

The Proxy pane (shown in Figure 37) displays the following information about each proxy LSAN device:

Port WWN   The WWN of the device port.

Proxy Fabric   The fabric ID of the edge fabric in which this device is a proxy.

Proxy PID   The port ID of the proxy device.

Physical Fabric   The fabric ID of the edge fabric in which this device physically exists.

Physical PID   The port ID of the corresponding physical device.

Node WWN   The WWN of the device node.

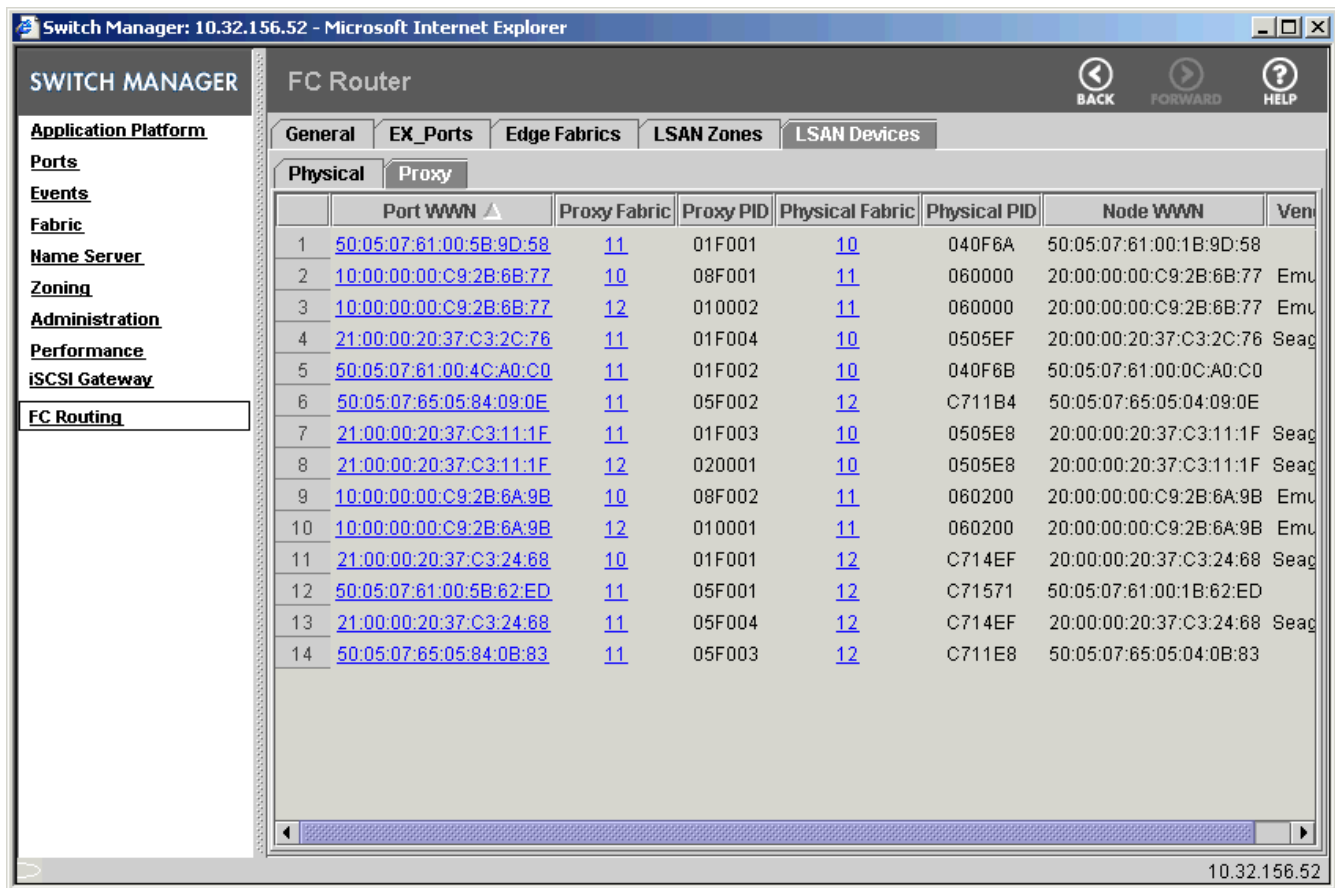Vendor   The name of the device vendor.

Figure 37 FC Routing page with LSAN Devices tab and Proxy subtab selected

Setting up a meta-SAN with an MP Router

Use the following procedure to set up a meta-SAN with an MP Router:

1. Stop all FCR ports (see "Starting and stopping a port" on page 51).
2. Connect the MP Routers to the edge fabrics and backbone fabric, if used.
3. Install or verify the Fibre Channel Routing Services license (see "Verifying, installing, and removing licenses" on page 34).
4. Configure EX_Ports (see "Configuring a port" on page 46).
5. Optional: Configure the backbone fabric, if you are planning to have one (see "Configuring a backbone fabric," next).
6. Establish LSAN zones in the edge fabrics.
7. Start all MP Router ports (see "Starting and stopping a port" on page 51).

Configuring a backbone fabric

Use this procedure to assign the fabric ID (FID) to a backbone fabric. The switch must be disabled first. If you do not disable the switch (see "Disabling an MP Router" on page 38), Advanced Web Tools disables and then re-enables the switch.

> **NOTE:** The fabric ID for a backbone fabric must be different from the fabric IDs of the edge fabrics.

Use the following procedure to configure a backbone fabric:

1. Access the Switch Manager.
2. Click **FC Routing** in the navigation bar.
3. Click the **General** tab.
4. Click **Set Fabric ID** in the task bar.
   The Set Backbone Fabric ID window opens.
5. Enter a fabric ID for the backbone fabric.
   The fabric ID is a number from 1 through 128.
6. Click **OK**.

10 Using exchange-based trunking

This chapter provides information on managing exchange-based trunking on a switch.

The trunking feature is disabled by default and can be enabled only after the trunking license is installed. Verify and install the trunking license using the procedures described in "Verifying, installing, and removing licenses" on page 34.

For background information on exchange-based trunking, see the *HP StorageWorks XPath OS 7.4.x administrator guide.*

Determining whether the trunking feature is enabled

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Trunking Information** tab.

   The Trunking tab pane indicates whether the trunking feature is enabled (see Figure 38).

> 📝 **NOTE:** The Trunking tab does not appear if the trunking license is not installed.

Enabling trunking on a switch

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Trunking Information** tab.
4. Click **Enable** in the task bar.
5. Click **Yes**.

   All Fibre Channel ports that passed the POST are enabled for trunking.

Disabling trunking on a switch

1. Access the Switch Manager.
2. Click **Administration** in the navigation bar.
3. Click the **Trunking Information** tab.
4. Click **Disable** in the task bar.
5. Click **Yes**.
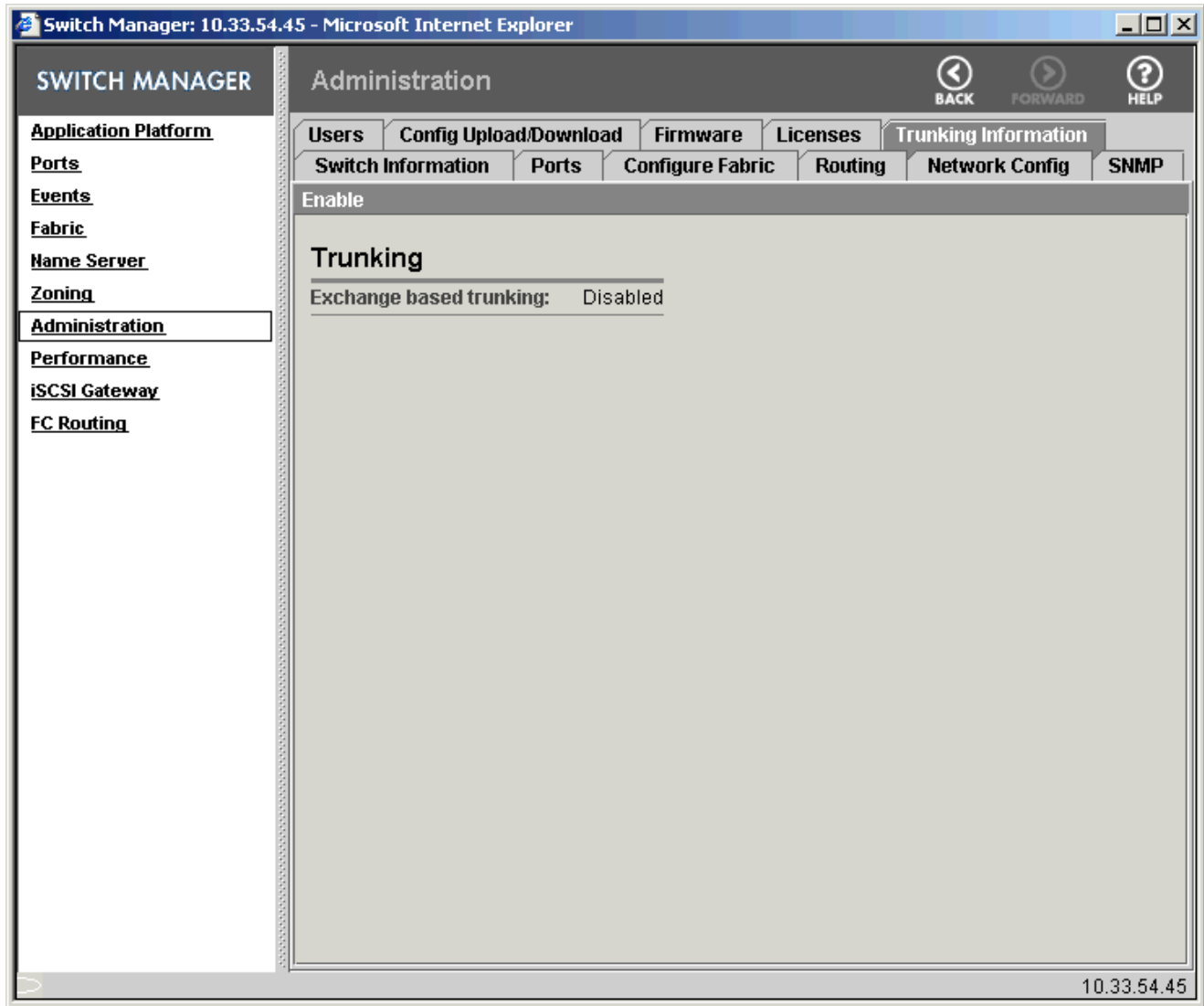
   All trunking on the switch is disabled.

Figure 38 Administration page with the Trunking Information tab selected

11 Managing the iSCSI Gateway

The HP iSCSI Gateway Service facilitates communication between TCP/IP networks and Fibre Channel SANs and displays iSCSI gateway configuration information across multiple MP Routers.

This chapter contains the following sections:

- Viewing and configuring iSCSI ports, next
- Viewing iSCSI device information, page 98
- Configuring an iSCSI gateway, page 99
- Creating an iSCSI initiator, page 100
- Deleting an iSCSI initiator, page 100
- Configuring CHAP, page 100
- Monitoring iSCSI performance, page 102

You can monitor and manage iSCSI through the Switch Manager. Click **iSCSI Gateway** in the navigation bar to access the iSCSI page.

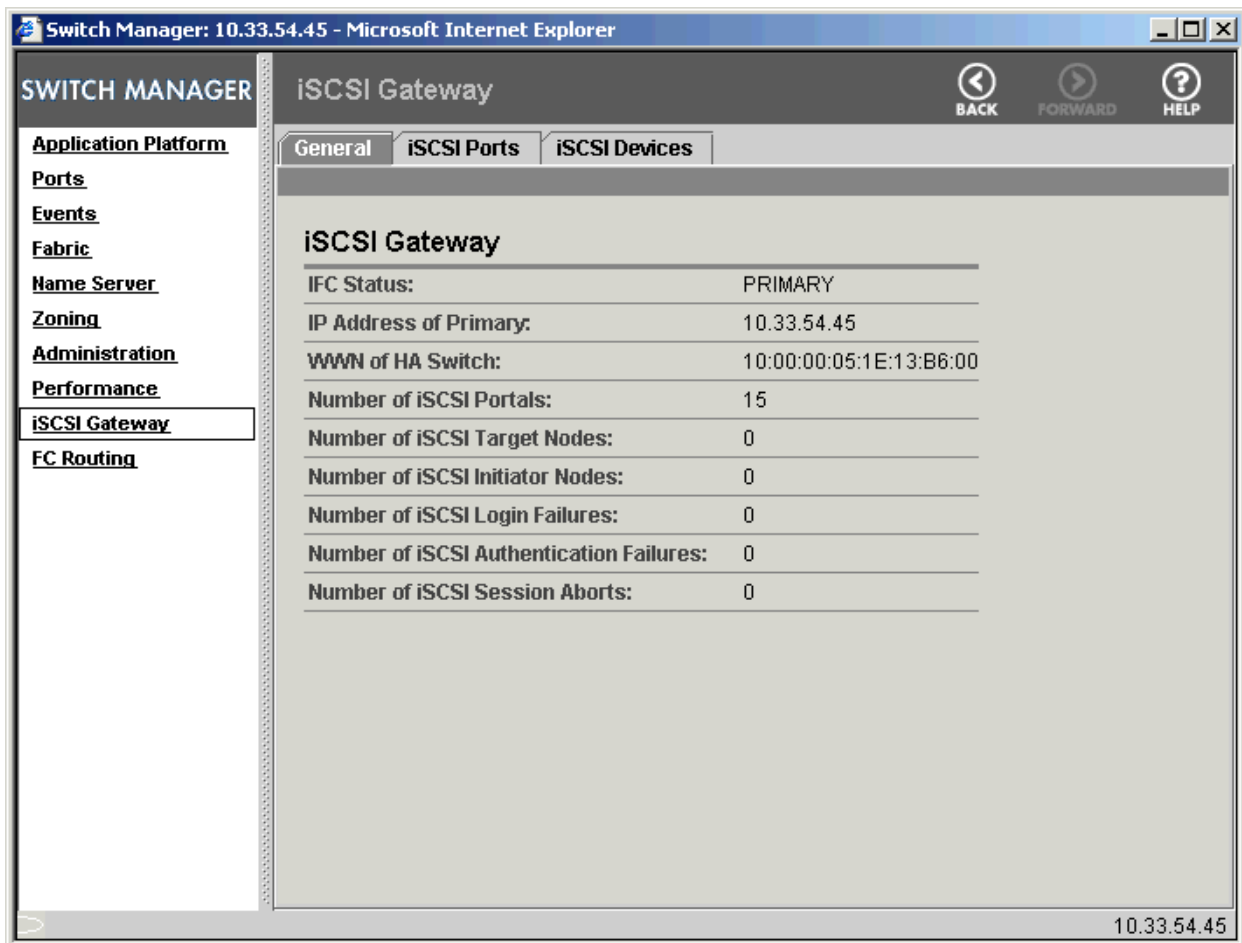The General tab displays basic iSCSI information. Figure 39 shows the iSCSI page with the General tab selected.

Figure 39 iSCSI Gateway page with General tab selected

Viewing and configuring iSCSI ports

The iSCSI Ports tab (see Figure 40) displays the iSCSI ports, including configuration and status information. You can also view this information from the Ports page.

To configure the iSCSI ports, use the same procedures described in "Managing ports" on page 45. The iSCSI port tasks that are listed in the task bar are the same as those tasks described in "Managing ports" on page 45.

For more detailed information on a specific port, click the port name to display a drill-down page for that port, as shown in Figure 4 on page 18. The name of the port is listed at the top of the page and is also indicated in the port diagram. The port drill-down page has several tabs that you can click to display additional information about the port.

You can perform port management tasks for a single port from the port drill-down page. You can perform these same tasks on multiple ports from the iSCSI Ports tab or the Ports page. These pages allow you to select multiple ports, for example, if you want to configure multiple ports at the same time.
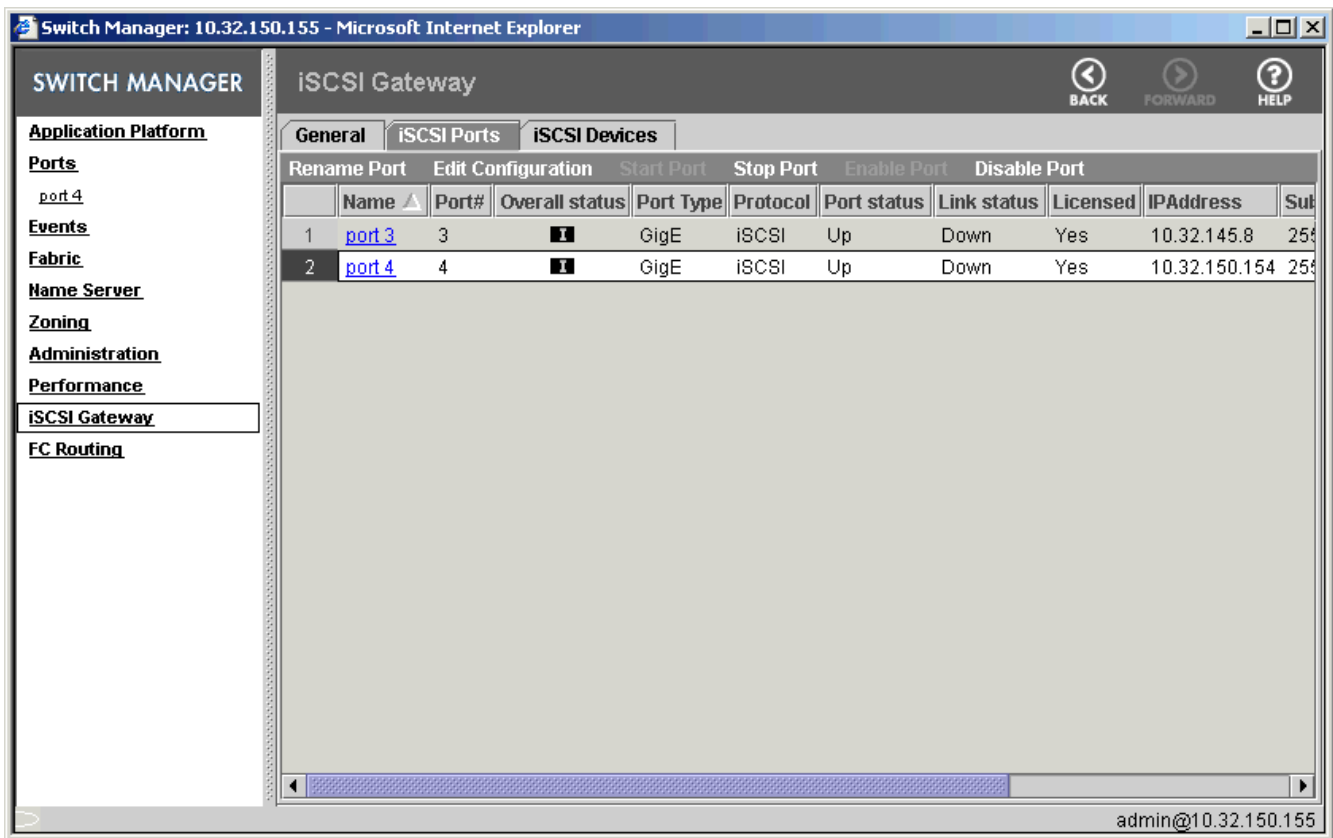
Figure 40 iSCSI Gateway page with ISCSI Ports tab selected

Viewing iSCSI device information

The iSCSI Devices tab (Figure 41) lists all the iSCSI names and provides the mapping between the iSCSI IQN and the Fibre Channel WWN. The table displays the following information about each iSCSI device:

iSCSI Name	The iSCSI name.
IP Address	The IP address of the iSCSI initiator.
Alias	The alias of the iSCSI initiator.
CHAP?	Indicates whether a CHAP secret has been configured.
Status	The status of the iSCSI device. Possible values are `Normal` and `Conflict`.
Vendor	The name of the device vendor.
Port WWN	The port WWN of the iSCSI initiator.

|	
Connected to	The domain and port that the iSCSI name translation is assigned (iSCSI port).
Initiator?	Indicates whether this is an initiator, a target, or unknown.
Physical?	Indicates whether this is a physical or a virtual device.
Transport	The type of transport used, such as iSCSI or FCP.
Symbolic Name	The symbolic name of Fibre Channel target.
Node WWN	The WWN of the iSCSI device.
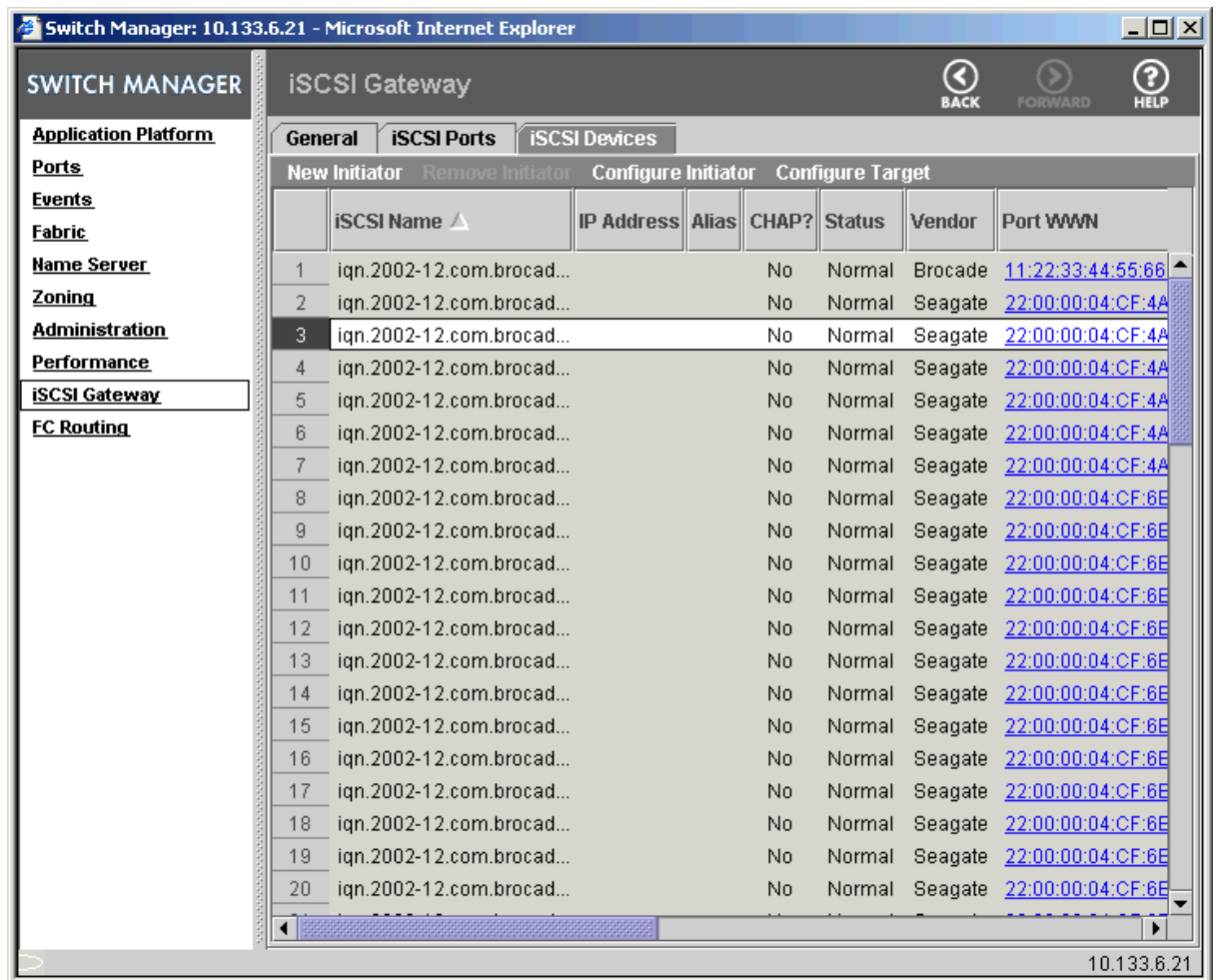
Figure 41 iSCSI Gateway page with Devices tab selected

Configuring an iSCSI gateway

The following is a four-step process for configuring an iSCSI gateway:

1. Create zones with the iSCSI initiators and the Fibre Channel targets as zone members.

   For information about creating zones, see "Managing zoning" on page 55.

   Create and manage the gateway zones the same way you create and manage any zones, but with two restrictions: A required naming convention distinguishes the iSCSI initiator members from other Fibre Channel zone members, and you use the port WWN name for the port connecting the Fibre Channel target to the fabric.

   For the iSCSI initiators, use iSCSI-standard fully qualified names (FQNs) in the IQN format, as in the following example:

   ```
   iqn.1991-05.com.microsoft:initiator1
   ```

   In this example, `iqn` is required, `1991-05.com.microsoft` indicates that the initiator is using the Microsoft® iSCSI driver, and `initiator1` is the name you assign to the initiator.

2. Optional: Zoning-based access control is required, but you can also use iSCSI shared secrets (that is, CHAP, access control) for enhanced security. If you choose to configure CHAP access control, see "Configuring CHAP" on page 100 to configure the shared secret for the Fibre Channel targets. When you configure the iSCSI initiator driver, you define the shared secret for the initiator.

3. Configure the iSCSI gateway ports using the procedure in "Configuring a port" on page 46.

4. Configure the iSCSI initiator driver.

   See the documentation from the iSCSI driver supplier for details for this step, but note that you typically need to add in the IP address for the iSCSI target portals. You set this address when you configure the iSCSI gateway ports. Next, you specify the Fibre Channel target names.

   If you are configuring CHAP for the initiators, do it at this time.

Creating an iSCSI initiator

Use the following procedure to create iSCSI initiators. You can, as an option, configure a CHAP secret at this time.

1. Access the Switch Manager of the primary IP configuration server.
2. Click **iSCSI Gateway** in the navigation bar.
3. Click the **iSCSI Devices** tab. (See Figure 41 on page 99.)
4. Click **New Initiator** in the task bar.

   The New iSCSI Initiator window opens.
5. Enter the name in the iSCSI Name box.
6. Optional: Enter a CHAP secret in the CHAP Secret box to create a CHAP secret for the new initiator.
7. Click **OK**.

Deleting an iSCSI initiator

Use the following procedure to delete iSCSI initiators:

1. Access the Switch Manager of the primary IP configuration server.
2. Click **iSCSI Gateway** in the navigation bar.
3. Click the **iSCSI Devices** tab. (See Figure 41 on page 99.)
4. Select the iSCSI initiator to delete.
5. Click **Remove Initiator** in the task bar.
6. Click **Yes** in the confirmation window.

Configuring CHAP

The iSCSI standard supports access control with CHAP. Using CHAP is optional. You can configure the iSCSI gateway to use one-way authentication, in which the target authenticates the host, or two-way authentication, in which first the target authenticates the host and then the host authenticates the target. You can also configure CHAP for iSCSI discovery sessions. In an iSCSI discovery session, the iSCSI host requests information about possible targets.

Configuring iSCSI initiators and CHAP secrets

1. Access the Switch Manager of the primary IP configuration server.
2. Click **iSCSI Gateway** in the navigation bar.
3. Click the **iSCSI Devices** tab. (See Figure 41 on page 99.)
4. Click **Configure Initiator** in the task bar.

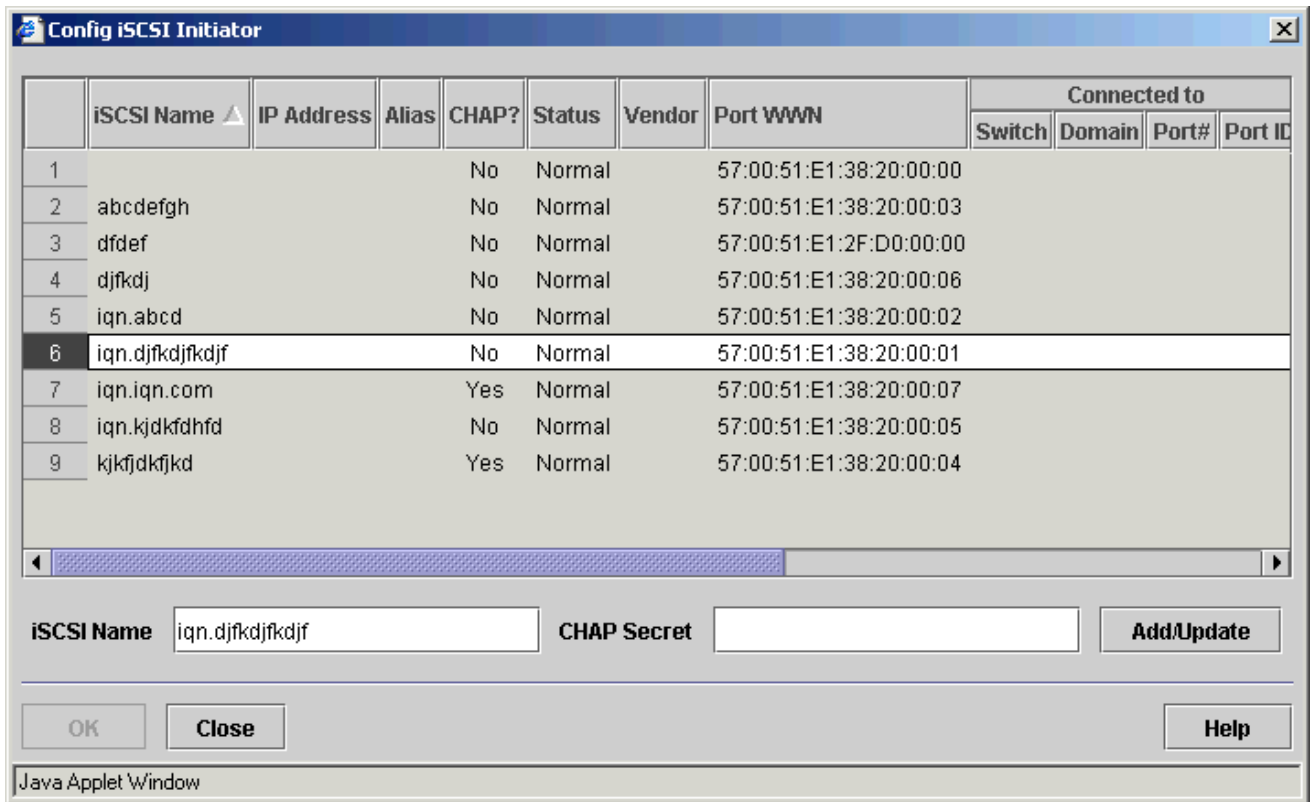   The Config iSCSI Initiator window opens (see Figure 42).

Figure 42 Config iSCSI Initiator window

5. To add an iSCSI initiator, enter the name in the iSCSI Name box and enter the CHAP secret in the CHAP Secret box.

   To add or modify the CHAP secret of an existing iSCSI initiator, select the name from the table at the top of the window, and enter the CHAP secret in the CHAP Secret box.

   To delete the CHAP secret of an existing iSCSI initiator, select the name from the table at the top of the window, and clear the CHAP secret in the CHAP Secret box.

   Remember the shared secret. Configure the iSCSI host side when you configure the iSCSI driver on the iSCSI host.

6. Click the **Add/Update** button.

7. Repeat step 5 and step 6 until you have finished configuring iSCSI initiators.

8. Click **Close**.

Configuring iSCSI targets and CHAP secrets

1. Access the Switch Manager of the primary IP configuration server.

2. Click **iSCSI Gateway** in the navigation bar.

3. Click the **iSCSI Devices** tab. (See Figure 41 on page 99.)

4. Click **Configure Target** in the task bar.

   The Config iSCSI Target window opens. (This window is similar to the Config iSCSI Initiator window, shown in Figure 42.)

5. To add an iSCSI target, enter the name in the iSCSI Name box and enter the CHAP secret in the CHAP Secret box.

   To add or modify the CHAP secret of an existing iSCSI target, select the name from the table at the top of the window and enter the CHAP secret in the CHAP Secret box.

   To delete the CHAP secret of an existing iSCSI target, select the name from the table at the top of the window and clear the CHAP secret in the CHAP Secret box.

   Remember the shared secret. Configure the iSCSI host side when you configure the iSCSI driver on the iSCSI host.

6. Click the **Add/Update** button.
7. Repeat step 5 and step 6 until you have finished configuring iSCSI targets.
8. Click **Close**.

Monitoring iSCSI performance

You can monitor the iSCSI performance through the Performance page by including iSCSI counters in performance charting. See "Monitoring performance" on page 83, for more information.

12 Notes on Advanced Web Tools

The following sections describe limitations and other information that you should be aware of:

- Browser limitations, next
- Java Plug-in limitations, page 103
- Online help issue, page 103

Browser limitations

The following is a known limitation in Advanced Web Tools, relevant to the browser:

Launching a telnet session from Advanced Web Tools on a Solaris or Linux system when using a Mozilla browser is not supported, due to technical limitations in Mozilla. Use an external telnet application to connect to the switch.

Java Plug-in limitations

The following are the known limitations in Advanced Web Tools, relevant to the Java Plug-in:

- When you launch Advanced Web Tools, if you click another switch in the fabric tree while the Switch Explorer is loading, a Java exception is generated and the application hangs. This can also happen if you refresh the browser while the applet is loading.

  To correct this situation, wait until the applet has finished loading and stabilizes before refreshing the browser or changing to another switch. If the application hangs, close and restart the browser.

- When you are running Advanced Web Tools on Solaris 2.8, Java Plug-in exceptions are generated if you click randomly within the fabric tree.

  To correct this situation, close and restart the browser. Do not click randomly on the fabric tree.

- When you are running Advanced Web Tools, a Java Plug-in exception is generated if you stop and start multiple ports repeatedly over a long period of time.

  To correct this situation, close and restart the browser.

Online help issue

Following is a known limitation in the Advanced Web Tools online help:

In the online help, sometimes the text in a table might be unreadable and appear to be overwritten by other text. In this case, click several times on the unreadable text, and the problem should clear up.

A   Summary of Switch Manager pages

This appendix lists the Switch Manager pages and tabs, and briefly describes what you can do on each page and tab.

Application page

Summary   View MP Router information.
                Turn the beacon on and off.
                Open a telnet window.

Details   View status of power supplies, temperature sensors, and fans.
                View configuration and status information for the MP Router module.

Ports page

(All tabs)   View and edit port configuration information.
                Rename port.
                Start and stop port.
                Enable and disable port.

Events page

View the event log.

Fabric page

View list of domains in the fabric and fabric topology.

Name Server page

All Devices   View list of all devices in the fabric.

Access Map   View access map of which targets and initiators can access each other, as defined by
                the enabled zone configuration.

Zoning page

Zone Server   Save all zone configuration information.
                Delete all zone configuration information.
                Enable or disable hard zoning.
                Enable or disable node WWN checking.

Zones   View list of zones in fabric.
                Create new zones.
                Delete, rename, and clone zones.
                Save all zone configuration information.

Zone Aliases	View list of zone aliases in fabric.
	Create new zone aliases.
	Delete, rename, and clone zone aliases.
	Save all zone configuration information.
Zone Configurations	View list of zone configurations in fabric.
	Create new zone configurations.
	Delete, rename, and clone zone configurations.
	Enable and disable zone configurations.
	Save all zone configuration information.

Administration page

Switch Information	Enable and disable MP Router.
	Reboot the MP Router.
	Rename the MP Router.
	Set the date and time.
	Change the domain ID.
Ports	View and edit port configuration information.
	Rename port.
	Start and stop port.
	Enable and disable port.
Configure Fabric	View fabric-related configuration parameters.
	Change domain ID and PID format.
Routing	Enable and disable in-order frame delivery and dynamic load sharing.
	View routing information.
	Add and delete static routes.
	Change link cost.
Network Config	View and edit management port configuration information.
	Add and delete syslog hosts.
SNMP	Edit SNMP parameters.
	Add, edit, and delete trap receivers.
Users	Manage user accounts.
Config Upload/Download	Backup and restore the configuration file.
Firmware	Download and install firmware packages.
Licenses	Add, delete, and view license keys.
Trunking Information	Enable and disable exchange-based trunking.

Performance page

| Counters | Display performance statistics for selected ports and counters. |
| Charts | Display performance graphs for selected ports and counters. |

iSCSI Gateway page

General	Display general information about the iSCSI gateway.
iSCSI Ports	View and edit iSCSI port configuration information. Rename iSCSI port. Start and stop iSCSI port. Enable and disable iSCSI port.
iSCSI Devices	View list of iSCSI initiators and targets. Add a new iSCSI initiator. Configure CHAP secrets for initiators or targets.

FC Routing page

General	Set the fabric ID.
EX_Ports	View and edit EX_Port configuration information. Rename EX_Port. Start and stop EX_Port. Enable and disable EX_Port.
Edge Fabrics	View information about all the attached edge fabrics.
LSAN Zones	View list of all LSAN zones in the edge fabrics.
LSAN Devices	View information about the physical and proxy LSAN devices.

B   Telnet command equivalents

If you are already familiar with the XPath OS telnet commands and want a quick reference as to how to perform the same function using Advanced Web Tools, see Table 4. This table lists XPath OS telnet commands and gives the corresponding Advanced Web Tools procedure. The commands are listed in alphabetical order.

For the commands for which there are no Advanced Web Tools equivalents, you can open a telnet window through Advanced Web Tools and run the commands from the telnet window.

All the available XPath OS telnet commands might not be listed in this table. For the definitive list of XPath OS telnet commands, see the *HP StorageWorks XPath OS 7.4.x command reference guide*.

Table 4   Telnet commands and Advanced Web Tools equivalents

Telnet command	Advanced Web Tools equivalent
agtCfgSet	Administration page, SNMP tab Click the **Edit** button in the SNMP table to edit the SNMP agent configuration. Click the **Add**, **Edit**, and **Remove** tasks in the Trap Receiver Entries table to manage the trap recipients. Both the telnet commands and Advanced Web Tools allow you to set the sysDescr, sysLocation, and sysContact variables. Through Advanced Web Tools, however, you can also set the sysName variable.
agtCfgShow	Administration page, SNMP tab View the SNMP table and the Trap Receiver Entries table.
aliAdd	Zoning page, Zone Aliases tab Click a zone alias name to open the zone alias drill-down page. Click the **Add Zone Alias Members** task.
aliCreate	Zoning page, Zone Aliases tab Click the **New** task.
aliDelete	Zoning page, Zone Aliases tab Select an alias and click the **Delete** task.
aliRemove	Zoning page, Zone Aliases tab Click an alias name to open the zone alias drill-down page. Select a member and click the **Remove Zone Alias Members** task.
aliShow	Zoning page, Zone Aliases tab You can view information about all zone aliases from this tab, or click a zone alias name to open the zone drill-down page for more detailed information about a specific zone alias.
altBoot	No corresponding Advanced Web Tools equivalent.
bannerSet	No corresponding Advanced Web Tools equivalent.
bannerShow	No corresponding Advanced Web Tools equivalent.
beacon	Application Platform page, Summary tab Click the **Turn Beacon On/Off** task.
burninErrShow	No corresponding Advanced Web Tools equivalent.
burninStatus	No corresponding Advanced Web Tools equivalent.
celloPortTest	No corresponding Advanced Web Tools equivalent.

Table 4 Telnet commands and Advanced Web Tools equivalents (continued)

Telnet command	Advanced Web Tools equivalent
cfgActvShow	Zoning page, Zone Configurations tab Click the effective zone configuration name to open the drill-down page.
cfgAdd	Zoning page, Zone Configurations tab Click a zone configuration name to open the drill-down page. Click the **Add Member** task.
cfgClear	Zoning page, Zone Server tab Click the **Purge** task.
cfgCreate	Zoning page, Zone Configurations tab Click the **New** task.
cfgDelete	Zoning page, Zone Configurations tab Select a configuration and click the **Delete** task.
cfgDisable	Zoning page, Zone Configurations tab Select the enabled configuration and click the **Disable** task.
cfgEnable	Zoning page, Zone Configurations tab Select a configuration and click the **Enable** task.
cfgRemove	Zoning page, Zone Configurations tab Click a zone configuration name to open the drill-down page. Select a member and click the **Remove Member** task.
cfgSave	Zoning page Click the **Save** task, which is available on any tab.
cfgShow	Zoning page, Zone Configurations tab
cfgSize	No corresponding Advanced Web Tools equivalent.
chassisShow	Application Platform page, Summary tab and Details tab
clear	No corresponding Advanced Web Tools equivalent.
configDefault	Administration page, Config Upload/Download tab Click the **Reset Configuration** task.
configDownload	Administration page, Config Upload/Download tab Click the **Download Configuration** task.
configShow	Administration page, Configure Fabric tab Administration page, Routing tab, Static Routes tab
configUpload	Administration page, Config Upload/Download tab Click the **Upload Configuration** task.
configure	Administration page, Configure Fabric tab Click the **Edit** button.
configureZoning	Zoning page, Zone Server tab Click the **Edit** button.
configZoningShow	Zoning page, Zone Server tab
crossPortTest	No corresponding Advanced Web Tools equivalent.
date	Administration page, Switch Information tab Click the **Set Date/Time** task.

Table 4 Telnet commands and Advanced Web Tools equivalents (continued)

Telnet command	Advanced Web Tools equivalent
diagDisablePost	No corresponding Advanced Web Tools equivalent.
diagEnablePost	No corresponding Advanced Web Tools equivalent.
diagHelp	No corresponding Advanced Web Tools equivalent.
diagPortMailbox	No corresponding Advanced Web Tools equivalent.
diagPortMem	No corresponding Advanced Web Tools equivalent.
diagPortMemArm	No corresponding Advanced Web Tools equivalent.
diagPost	No corresponding Advanced Web Tools equivalent.
diagSetBurnin	No corresponding Advanced Web Tools equivalent.
diagSetCycle	No corresponding Advanced Web Tools equivalent.
diagStopBurnin	No corresponding Advanced Web Tools equivalent.
diagUpload	No corresponding Advanced Web Tools equivalent.
dlsReset	Administration page, Routing tab, IOD/DLS subtab Click the **Edit** button.
dlsSet	Administration page, Routing tab, IOD/DLS subtab Click the **Edit** button.
dlsShow	Administration page, Routing tab, IOD/DLS subtab
errClear	No corresponding Advanced Web Tools equivalent.
errShow	No corresponding Advanced Web Tools equivalent.
eventActionSet	No corresponding Advanced Web Tools equivalent.
eventActionShow	No corresponding Advanced Web Tools equivalent.
eventClear	No corresponding Advanced Web Tools equivalent.
eventLogSize	No corresponding Advanced Web Tools equivalent.
eventSeverity	No corresponding Advanced Web Tools equivalent.
eventSeverityShow	No corresponding Advanced Web Tools equivalent.
eventShow	Events page Click the **ShowAll** task.
eventShowByNum	No corresponding Advanced Web Tools equivalent.
exit	No corresponding Advanced Web Tools equivalent.
fabLogClear	No corresponding Advanced Web Tools equivalent.
fabLogShow	No corresponding Advanced Web Tools equivalent.
fabricShow	Fabric page
fanShow	From the Switch Explorer, click the **Fan** button. From the Switch Manager Application Platform page, click the **Details** tab.
fastBoot	Administration page, Switch Information tab Click the **Reboot** task.
fazoneAdd	Zoning page, Zones tab Click a zone name to open the drill-down page. Click the **Add Members** task.

Table 4 Telnet commands and Advanced Web Tools equivalents (continued)

Telnet command	Advanced Web Tools equivalent
fazoneCreate	Zoning page, Zones tab Click the **New** task.
fazoneDelete	Zoning page, Zones tab Select a zone and click the **Delete** task.
fazoneRemove	Zoning page, Zones tab Click a zone name to open the drill-down page. Select a member and click the **Remove Members** task.
fazoneShow	Zoning page, Zones tab
fcipShow	Ports page, FCIP Ports tab Click a port name to open the drill-down page.
fcrConfigure	FC Routing page, General tab Click the **Set Fabric ID** task.
fcrFabricShow	No corresponding Advanced Web Tools equivalent.
fcrPhyDevShow	FC Routing page, LSAN Devices tab, Physical subtab
fcrProxyConfig	No corresponding Advanced Web Tools equivalent.
fcrProxyDevShow	FC Routing page, LSAN Devices tab, Proxy subtab
fcrResourceShow	No corresponding Advanced Web Tools equivalent.
fcrRouteShow	No corresponding Advanced Web Tools equivalent.
fcrXlateConfig	No corresponding Advanced Web Tools equivalent.
firmwareCommit	No corresponding Advanced Web Tools equivalent.
firmwareDownload	Administration page, Firmware tab Click the **Download** task.
firmwareShow	Administration page, Firmware tab
fspfShow	No corresponding Advanced Web Tools equivalent.
h	No corresponding Advanced Web Tools equivalent.
help	No corresponding Advanced Web Tools equivalent.
ifcsDisable	No corresponding Advanced Web Tools equivalent.
ifcsEnable	No corresponding Advanced Web Tools equivalent.
ifcsShow	No corresponding Advanced Web Tools equivalent.
ifModeShow	No corresponding Advanced Web Tools equivalent.
interfaceShow	No corresponding Advanced Web Tools equivalent.
iodReset	Administration page, Routing tab, IOD/DLS subtab Click the **Edit** button.
iodSet	Administration page, Routing tab, IOD/DLS subtab Click the **Edit** button.
iodShow	Administration page, Routing tab, IOD/DLS subtab
ipaddrSet	Administration page, Network Config tab Click the **Edit** button.

Table 4 Telnet commands and Advanced Web Tools equivalents (continued)

Telnet command	Advanced Web Tools equivalent
`ipaddrShow`	Administration page, Network Config tab
`iscsiAuthCfg`	iSCSI Gateway page, General tab
`iscsiFailoverAdd`	No corresponding Advanced Web Tools equivalent.
`iscsiFailoverDelete`	No corresponding Advanced Web Tools equivalent.
`iscsiPortShow`	For port statistics: Performance page, Counters tab. Click **Select Ports and Counters** to configure iSCSI ports and performance counters.
`iscsiShow`	iSCSI Gateway page, General tab
`iscsiWwnAlloc`	iSCSI Gateway page, Devices tab
`licenseAdd`	Administration page, Licenses tab Click the **Add** task.
`licenseRemove`	Administration page, Licenses tab Select a license and click the **Remove** task.
`licenseShow`	Administration page, Licenses tab
`linkCost`	Administration page, Routing tab, Link Cost subtab Select a port and click the **Edit** task.
`lsanZoneShow`	FC Routing page, LSAN Zones tab Click a zone name to open the drill-down page.
`lsdbShow`	No corresponding Advanced Web Tools equivalent.
`nbrStateShow`	No corresponding Advanced Web Tools equivalent.
`nbrStatsClear`	No corresponding Advanced Web Tools equivalent.
`nsAllShow`	Name Server page, All Devices tab
`nsShow`	Name Server page, All Devices tab
`passwd`	Administration page, Users tab Select your user name and click the **Change Your Password** task.
`pdShow`	No corresponding Advanced Web Tools equivalent.
`ping`	No corresponding Advanced Web Tools equivalent.
`pkiShow`	No corresponding Advanced Web Tools equivalent.
`portCfgDefault`	No corresponding Advanced Web Tools equivalent.
`portCfgEPort`	Ports page, All Ports tab Select a port and click the **Edit Configuration** task.
`portCfgEXPort`	Ports page, All Ports tab Select a port and click the **Edit Configuration** task.
`portCfgFcip`	Ports page, FCIP Ports tab
`portCfgGige`	Ports page, FCIP Ports tab
`portCfgLongDistance`	Ports page, FC Ports tab Select a port and click the **Edit Configuration** task.

Table 4 Telnet commands and Advanced Web Tools equivalents (continued)

Telnet command	Advanced Web Tools equivalent
portCfgNPort	Ports page, All Ports tab Select a port and click the **Edit Configuration** task.
portCfgSpeed	Ports page, FC Ports tab Select a port and click the **Edit Configuration** task.
portCfgTopology	Ports page, FC Ports tab Select a port and click the **Edit Configuration** task.
portDiagClear	No corresponding Advanced Web Tools equivalent.
portDiagDisable	No corresponding Advanced Web Tools equivalent.
portDiagEnable	No corresponding Advanced Web Tools equivalent.
portDisable	Ports page, All Ports tab Select a port and click the **Disable Port** task.
portEnable	Ports page, All Ports tab Select a port and click the **Enable Port** task.
portErrShow	No corresponding Advanced Web Tools equivalent.
portLogClear	No corresponding Advanced Web Tools equivalent.
portLogDisable	No corresponding Advanced Web Tools equivalent.
portLogDump	No corresponding Advanced Web Tools equivalent.
portLogEnable	No corresponding Advanced Web Tools equivalent.
portLogShow	No corresponding Advanced Web Tools equivalent.
portLoopbackTest	No corresponding Advanced Web Tools equivalent.
portName	Ports page, All Ports tab Select a port and click the **Rename Port** task.
portPerfShow	Performance page, Counters or Charts tab
portRouteInfo	No corresponding Advanced Web Tools equivalent.
portShow	Port drill-down page, General tab
portStart	Ports page, All Ports tab Select a port and click the **Start Port** task.
portStatsShow	Port drill-down page, Port Statistics tab.
portStop	Ports page, All Ports tab Select a port and click the **Stop Port** task.
portType	Ports page, All Ports tab Select a port and click the **Edit Configuration** task.
ps	No corresponding Advanced Web Tools equivalent.
psShow	Application Platform page, Summary tab and Details tab
qloopAdd	No corresponding Advanced Web Tools equivalent.
qloopCreate	No corresponding Advanced Web Tools equivalent.
qloopDelete	No corresponding Advanced Web Tools equivalent.
qloopRemove	No corresponding Advanced Web Tools equivalent.

Table 4 Telnet commands and Advanced Web Tools equivalents (continued)

Telnet command	Advanced Web Tools equivalent
qloopShow	No corresponding Advanced Web Tools equivalent.
quit	No corresponding Advanced Web Tools equivalent.
reboot	Administration page, Switch Information tab Click the **Reboot** task.
rnPing	No corresponding Advanced Web Tools equivalent.
routeShow	No corresponding Advanced Web Tools equivalent.
secAuthSecret	No corresponding Advanced Web Tools equivalent.
serviceCfg	No corresponding Advanced Web Tools equivalent.
setFanSpeed	No corresponding Advanced Web Tools equivalent.
setPagerOff	No corresponding Advanced Web Tools equivalent.
setPagerOn	No corresponding Advanced Web Tools equivalent.
sfpShow	Port drill-down page, SFP tab
sfpSupport	No corresponding Advanced Web Tools equivalent.
showRecovery	No corresponding Advanced Web Tools equivalent.
spinSilk	No corresponding Advanced Web Tools equivalent.
supportShow	No corresponding Advanced Web Tools equivalent.
svipAddrSet	Administration page, Network Config tab Click the **Edit** button.
svipAddrShow	Administration page, Network Config tab
switchDisable	Administration page, Switch Information tab Click the **Disable** task.
switchEnable	Administration page, Switch Information tab Click the **Enable** task.
switchName	Administration page, Switch Information tab Click the **Rename** task.
switchShow	Application Platform page, Summary tab
switchStatusShow	Switch Explorer: Status button
syslogdipAdd	Administration page, Network Config tab Click the **Add** task.
syslogdipRemove	Administration page, Network Config tab Click the **Delete** task.
syslogdipShow	Administration page, Network Config tab
tempShow	Switch Explorer: Temp button Switch Manager: Application Platform page, Details tab
timeout	No corresponding Advanced Web Tools equivalent.
timeZoneSet	Administration page, Switch Information tab Click the **Set Date/Time** task.
top	No corresponding Advanced Web Tools equivalent.

Table 4 Telnet commands and Advanced Web Tools equivalents (continued)

Telnet command	Advanced Web Tools equivalent
topologyShow	Fabric page
trunkReset	Administration page, Trunking tab Click the **Disable** task.
trunkSet	Administration page, Trunking tab Click the **Enable** task.
trunkShow	Administration page, Trunking tab
tsClockServer	No corresponding Advanced Web Tools equivalent.
upTime	Administration page, Switch Information tab See **Boot Time** in the Switch table.
urouteConfig	Administration page, Routing tab, Static Routes subtab Click the **Add** task.
urouteRemove	Administration page, Routing tab, Static Routes subtab Select a route and click the **Delete** task.
urouteShow	Administration page, Routing tab, FSPF Routes subtab
userAdd	Administration page, **Users** tab Click the **Add User** task.
userDel	Administration page, Users tab Select a user and click the **Delete User** task.
users	No corresponding Advanced Web Tools equivalent.
userShow	Administration page, Users tab
version	Administration page, Firmware tab
wdogevt	No corresponding Advanced Web Tools equivalent.
zoneAdd	Zoning page, Zones tab Click a zone name to open the drill-down page. Click the **Add Members** task.
zoneCreate	Zoning page, Zones tab Click the **New** task.
zoneDelete	Zoning page, Zones tab Select a zone and click the **Delete** task.
zoneRemove	Zoning page, Zones tab Click a zone name to open the drill-down page. Select a member and click the **Remove Members** task.
zoneShow	Zoning page, Zones tab Click a zone name to open the drill-down page.
zsdLogClear	No corresponding Advanced Web Tools equivalent.
zsdLogShow	No corresponding Advanced Web Tools equivalent.

Glossary

alias

A logical grouping of elements in a fabric. An alias is a collection of port numbers and connected devices, used to simplify the entry of port numbers and WWNs when creating zones.

area number

In Fabric OS 4.0 and later, ports on a switch are assigned a logical area number. Port area numbers can be viewed by issuing the `switchShow` command. They are used to define the operative port for many Fabric OS commands, for example, area numbers can be used to define the ports within an alias or zone.

ASIC

Application-specific integrated circuit.

authentication

The process of verifying that an entity in a fabric (such as a switch) is what it claims to be.

backbone fabric

An optional capability that enables scalable meta-SANs by allowing the networking of multiple FC routers, which connect to the backbone fabric through EB_Port interfaces.

BB_Credit

Buffer-to-buffer credit. The number of frames that can be transmitted to a directly connected recipient or within an arbitrated loop. Determined by the number of receive buffers available.

beacon

A tool in which all the port LEDs on a switch are set to flash from one side of the switch to the other, to enable identification of an individual switch in a large fabric. A switch can be set to beacon by a CLI command or through Advanced Web Tools.

CHAP

Challenge-Handshake Authentication Protocol. Allows remote servers and clients to securely exchange authentication credentials. Both the server and client are configured with the same shared secret.

chassis

The metal frame in which the switch and switch components are mounted.

circuit

An established communication path between two ports. Consists of two virtual circuits capable of transmitting in opposite directions.

CLI

Command line interface. An interface that depends entirely on the use of commands, such as through telnet or SNMP, and does not involve a GUI.

client

An entity that, using its common transport (CT), makes requests of a server.

community (SNMP)

A relationship between a group of SNMP managers and an SNMP agent, in which authentication, access control, and proxy characteristics are defined. *See also* SNMP.

configuration

1. A set of parameters that can be modified to fine-tune the operation of a switch. Use the `configshow` command to view the current configuration of the switch.

2. In HP StorageWorks Zoning, a zoning element that contains a set of zones. The configuration is the highest-level zoning element and is used to enable or disable a set of zones on the fabric. *See also* zone configuration.

core PID

Core switch port identifier. The core PID must be set for Fabric OS 3.1 and earlier switches included in a fabric of Fabric OS 4.1 switches. This parameter is located in the `configure` command of firmware versions 3.1 and earlier. All version 4.1 switches and later use the core PID format by default; this parameter is not present in the `configure` command for these switches.

credit

In Fibre Channel technology, the number of receive buffers available to transmit frames between ports. *See also* BB_Credit.

defined zone configuration

The set of all zone objects defined in the fabric. Can include multiple zone configurations. *See also* error, zone configuration.

D_ID

Destination identifier. A three-byte field in the frame header that indicates the address identifier of the N_Port to which the frame is headed.

director

An HP StorageWorks Core Switch 2/64, SAN Director 2/128, or 4/256 SAN Director.

DLS

Dynamic load-sharing. Dynamic distribution of traffic over available paths. Allows for the recomputing of routes when an Fx_Port or an E_Port changes status.

domain ID

A unique identifier for all switches in a fabric, used in routing frames. Usually assigned by the principal switch, but can be assigned manually. The domain ID for an HP StorageWorks switch can be any integer from 1 through 239.

edge fabric

A Fibre Channel fabric connected to an FC router through an EX_Port (where hosts and storage are attached in a meta-SAN).

E_D_TOV

Error-detect timeout value. The minimum time a target waits for a sequence to complete before initiating recovery. Can also be defined as the maximum time allowed for a round-trip transmission before an error is declared. *See also* R_A_TOV.

enabled zone configuration

The currently enabled configuration of zones. Only one configuration can be enabled at a time. *See also* defined zone configuration, zone configuration.

E_Port

Expansion port. A standard Fibre Channel mechanism that enables switches to network with each other, creating an ISL. *See also* ISL.

error

With respect to the Fibre Channel industry, a missing or corrupted frame, timeout, loss of synchronization, or loss of signal (link errors).

EX_Port

A type of E_Port that connects an FC router to an edge fabric. EX_Ports limit the scope of fabric services, but provide device connectivity using FC-NAT.

fabric

A collection of Fibre Channel switches and devices, such as hosts and storage. Also called a *switched fabric*. *See also* SAN, topology.

fabric services

Codes that describe the communication to and from any well-known address.

fabric topology

The arrangement of switches that form a fabric.

FC router

A platform running the HP Fibre Channel Routing Service or FC-to-FC Routing (for instance, the MP Router) that enables two or more fabrics to share resources (such hosts or storage devices) without merging those fabrics. The MP Router could simultaneously be used as an FC router and as an FCIP tunnel or iSCSI gateway.

FC-GS-3

Fibre Channel Generic Services, third generation.

FCIP

Fibre Channel over IP.

FCIP Tunneling Service

The HP StorageWorks Multi-protocol SAN Routing Service that enables SANs to span longer distances than could be supported with native Fibre Channel links. FCIP is a TCP/IP-based tunneling protocol that allows the transparent interconnection of geographically distributed SAN islands through an IP-based network.

FCP

Fibre Channel Protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FC-SW-2

The second-generation Fibre Channel Switch Fabric standard defined by ANSI. Specifies tools and algorithms for the interconnection and initialization of Fibre Channel switches to create a multiswitch Fibre Channel fabric.

Fibre Channel

The primary protocol used for building SANs to transmit data between servers, switches, and storage devices. Unlike IP and Ethernet, Fibre Channel is designed to support the needs of storage devices of all types. It is a high-speed, serial, bidirectional, topology-independent, multi-protocol, and highly scalable interconnection between computers, peripherals, and networks.

FID

Fabric ID. Unique identifier of a fabric in a meta-SAN.

firmware

The basic operating system provided with the hardware.

FL_Port

Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated-loop capabilities. Can be used to connect an NL_Port to a switch. *See also* F_Port, Fx_Port.

F_Port

Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. *See also* FL_Port, Fx_Port.

frame

The Fibre Channel structure used to transmit data between ports. Consists of a start-of-frame delimiter, header, optional headers, data payload, cyclic redundancy check (CRC), and end-of-frame delimiter. There are two types of frames: link control frames (transmission acknowledgements, and so forth) and data frames.

FSPF

Fabric shortest path first. The HP routing protocol for Fibre Channel switches.

FTP

File Transfer Protocol.

Fx_Port

A fabric port that can operate as either an F_Port or FL_Port. *See also* F_Port, FL_Port.

gateway

Hardware that connects incompatible networks by providing translation for both hardware and software. For example, an ATM gateway can be used to connect a Fibre Channel link to an ATM connection.

Gbit/sec

Gigabits per second (1,062,500,000 bits per second).

GBIC

Gigabit interface converter. A removable serial transceiver module that allows gigabaud physical-level transport for Fibre Channel and gigabit Ethernet.

HBA

Host bus adapter. The interface card between a server or workstation bus and the Fibre Channel network.

host

A computer system that provides end users with services like computation and storage access.

IFL

Interfabric link. A connection between a router and an edge fabric. Architecturally, these can be of type EX_Port-to-E_Port or EX_Port-to-EX_Port.

initiator

A server or workstation on a Fibre Channel network that initiates communications with storage devices. *See also* target.

interswitch link

See ISL.

IOD

In-order delivery. A parameter that, when set, guarantees that frames are either delivered in order or dropped.

IP

Internet Protocol. The addressing part of TCP.

IQN

iSCSI qualified name.

iSCSI

Internet Small Computer Systems Interface. A protocol that defines the processes for transferring block storage applications over TCP/IP networks by encapsulating SCSI commands into TCP and transporting them over the network by IP. *See also* SCSI.

iSCSI Gateway Service

The HP Multi-protocol SAN Routing Service that maps the FCP protocol to the IP transport. This service projects iSCSI hosts onto the backbone fabric of a gateway switch.

ISL

Interswitch link. A Fibre Channel link from the E_Port of one switch to the E_Port of another. *See also* E_Port.

JBOD

Just a bunch of disks. A number of disks connected in a single chassis to one or more controllers. *See also* RAID.

LED

Light-emitting diode. Used to indicate the status of elements on a switch.

Loop Mode

One of two possible modes for an L_Port, in which the L_Port is in an arbitrated loop, using loop protocol. An L_Port in Loop Mode can also be in Participating Mode or Nonparticipating Mode.

LSAN

Logical storage area network. An LSAN enables device and storage connectivity that spans two or more fabrics. The path between devices in an LSAN can be local to a fabric or cross one or more FC routers and one or more backbone fabrics.

LSAN zone

The mechanism by which LSANs are administered. An FC router attached to two fabrics listens for the creation of matching LSAN zones on both fabrics. If this occurs, it creates phantom domains and FC-NAT entries as appropriate, and inserts entries for them into the name servers on the fabrics. LSAN zones are compatible with all standard zoning mechanisms.

Mbit/sec

Megabits per second.

meta-SAN

The collection of all devices, switches, edge and backbone fabrics, LSANs, and FC routers that make up a physically connected but logically partitioned storage network. LSANs span between edge fabrics using FC routers. In a data network, this would simply be called *the network*. However, an additional term is required to specify the difference between a single-fabric network (SAN), a multifabric network without cross-fabric connectivity (dual-redundant fabric SAN), and a multifabric network with connectivity (meta-SAN).

metric

A relative value assigned to a route to aid in calculating the shortest path (1000 at 1–Gbit/sec, 500 at 2–Gbit/sec).

MIB

Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

Name Server

Simple Name Server (SNS). A switch service that stores names, addresses, and attributes for up to 15 minutes and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. Also called a *directory service*.

node

A Fibre Channel device that contains an N_Port or NL_Port. *See also* N_Port.

N_Port

Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection.

NS

Name Server. The service provided by a fabric switch that stores names, addresses, and attributes related to Fibre Channel objects. Can cache information for up to 15 minutes. Also called a *Simple Name Server* or a *directory service*.

Nx_Port

A node port that can operate as either an N_Port or NL_Port. *See also* N_Port.

originator

The Nx_Port that originated an exchange.

payload

A Fibre Channel frame has a header and a payload. The payload contains the information being transported by the frame; it is determined by the higher-level service or FC_4 upper-level protocol. There are many different payload formats, based on protocol.

PID

Port identifier. *See also* core PID.

point-to-point

A Fibre Channel topology that employs direct links between each pair of communicating entities. *See also* topology.

port

In an HP StorageWorks switch environment, an SFP or GBIC receptacle on a switch to which an optical cable for another device is attached.

port name

A user-defined alphanumeric name for a port.

POST

Power-on self-test. A series of tests run by a switch after it is turned on.

principal switch

The first switch to boot up in a fabric. Ensures unique domain IDs among roles.

protocol

A defined method and set of standards for communication. Determines the type of error-checking, the data-compression method, how sending devices indicate an end of message, and how receiving devices indicate receipt of a message.

RAID

Redundant array of independent disks. A collection of disk drives that appear as a single volume to the server and are fault tolerant through mirroring or parity checking. *See also* JBOD.

R_A_TOV

Resource allocation timeout value. The maximum time a frame can be delayed in the fabric and still be delivered. *See also* E_D_TOV.

receiver

A device that performs detection and signal processing.

route

With respect to a fabric, the communication path between two switches. Might also apply to the specific path taken by an individual frame, from source to destination. *See also* FSPF.

routing

The assignment of frames to specific switch ports, according to frame destination.

SAN

Storage area network. A network of systems and storage devices that communicate using Fibre Channel protocols. *See also* fabric.

SCSI

Small Computer Systems Interface. A parallel bus architecture and a protocol for transmitting large data blocks to a distance of 15 to 25 meters. *See also* iSCSI, iSCSI Gateway Service.

server

A computer that processes end-user applications or requests.

SFP

Small-form-factor pluggable. A transceiver used on 2–GB/sec switches that replaces the GBIC.

S_ID

Source ID. Refers to the native port address (24–bit address).

SNMP

Simple Network Management Protocol. An Internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols. *See also* community (SNMP).

switch name

The arbitrary name assigned to a switch.

switch port

A port on a switch. Switch ports can be E_Ports, F_Ports, or FL_Ports. *See also* E_Port, F_Port, FL_Port.

syslog

Syslog daemon. Used to forward error messages.

T11

A standards committee chartered with creating standards for Fibre Channel.

target

A storage device on a Fibre Channel network. *See also* initiator.

TCP/IP

Transmission Control Protocol Internet Protocol. A communications protocol developed under contract from the U.S. Department of Defense to internetwork dissimilar systems.

telnet

A virtual terminal emulation used with TCP/IP. *Telnet* is sometimes used as a synonym for the HP StorageWorks Fabric OS CLI.

topology

In Fibre Channel technology, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- Point to point: A direct link between two communication ports.
- Switched fabric: Multiple N_Ports linked to a switch by F_Ports.
- Arbitrated loop: Multiple NL_Ports connected in a loop.

translate domain

A router virtual domain that represents an entire fabric. Device connectivity can be achieved from one fabric to another, over the router and through this virtual domain, without merging the two fabrics. Also known as *phantom domains*.

trap (SNMP)

The message sent by an SNMP agent to inform the SNMP management station of a critical error. *See also* SNMP.

trunking

In Fibre Channel technology, a feature that enables distribution of traffic over the combined bandwidth of up to four ISLs between adjacent switches, while preserving in-order delivery.

tunneling

A technique for enabling two networks to communicate when the source and destination hosts are both on the same type of network but are connected by a different type of network.

U_Port

Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or FL_Port. A port is defined as a U_Port when it is not connected or has not yet assumed a specific function in the fabric.

WWN

World wide name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

zone

A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access to others in the zone but are not visible to any outside the zone.

zone configuration

A specified set of zones. Enabling a configuration enables all zones in that configuration. *See also* defined zone configuration, error.

zoning

A feature in fabric switches or hubs that allows segmentation of a node by physical port, name, or address.

Index